538,289

(12)特許協力条約に基づいて公開された国際出願

10 JUN 2005

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年7 月1 日 (01.07.2004)

PCT

(10) 国際公開番号
WO 2004/055685 A1

(51) 国際特許分類[7]: G06F 15/00, 12/00, 12/14

(21) 国際出願番号: PCT/JP2003/016130

(22) 国際出願日: 2003 年12 月16 日 (16.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2002-366489
2002 年12 月18 日 (18.12.2002) JP

(71) 出願人 (米国を除く全ての指定国について): インターナショナル・ビジネス・マシーンズ・コーポレーション (INTERNATIONAL BUSINESS MACHINES CORPORATION) [US/US]; 10504 ニューヨーク州 アーモンク ニュー オーチャード ロード NY (US).

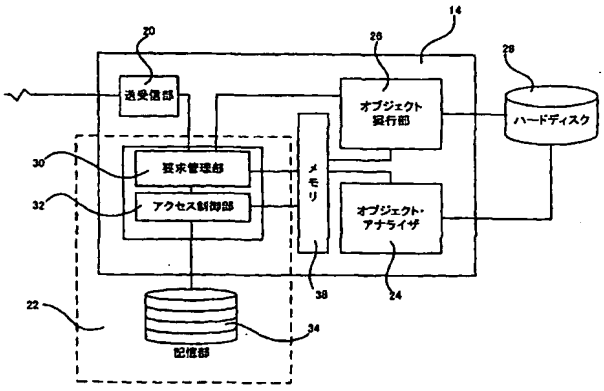
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 立堀 道昭 (TATSUBORI,Michiaki) [JP/JP]; 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kanagawa (JP). 高瀬 俊郎 (TAKASE,Toshiroh) [JP/JP]; 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kanagawa (JP). 中村 祐一 (NAKAMURA,Yuhichi) [JP/JP]; 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内 Kanagawa (JP).

[続葉有]

(54) Title: WEB SERVICE PROVIDING SYSTEM, SERVER DEVICE FOR THE SAME, CONTROL METHOD FOR CONTROLLING COMPUTER SYSTEM AS SERVER DEVICE FOR WEB SERVICE PROVIDING SYSTEM, PROGRAM FOR EXECUTING THE CONTROL METHOD, AND RECORDING MEDIUM

(54) 発明の名称: Webサービス提供システム、そのためのサーバ装置、コンピュータ・システムをWebサービス提供システムのためのサーバ装置として制御するための制御方法、および該制御方法を実行するためのプログラムおよび記録媒体



20...TRANSMISSION/RECEPTION SECTION
30...REQUEST MANAGEMENT SECTION
32...ACCESS CONTROL SECTION
38...MEMORY
26...OBJECT EXECUTION SECTION
24...OBJECT ANALYZER
28...HARD DISC
34...STORAGE SECTION

(57) Abstract: There are provided a Web service providing system, a server device for it, a control method for controlling a computer system as a server device for the Web service providing system, a program for executing the control method, and a recording medium. The Web service providing system includes a server device (14). The server device (14) has an object analyzer (24) for acquiring all the methods which may be called out by a request object and generating an access authority set, object execution means (26) for executing a request object, and a storage section (34) for storing the execution result of a past object. Furthermore, the server device (14) has a cache mechanism (22) for executing access control for the storage section (34) in response to an object call request by using the access authority set.

(57) 要約: Webサービス提供システム、そのためのサーバ装置装置、コンピュータ・システムをWebサービス提供システムのためのサーバ装置装置として制御するための制御方法、および該制御方法を実行するためのプログラムおよび記録媒体を提供する。 本発明のWebサービス提

[続葉有]

WO 2004/055685 A1

(74) 代理人: 坂口 博, 外(SAKAGUCHI,Hiroshi et al.); 〒242-8502 神奈川県 大和市 下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内 Kanagawa (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

供システムは、サーバ装置装置１４を含んで構成される。サーバ装置装置１４は、要求オブジェクトが呼出す可能性のあるメソッドすべてを取得してアクセス権限セットを生成するオブジェクト・アナライザ２４と、要求オブジェクトを実行するためのオブジェクト実行手段２６と、過去のオブジェクトの実行結果を格納する記憶部３４を含んで構成され、かつアクセス権限セットを使用してオブジェクト呼出し要求に応答して記憶部３４に対するアクセス制御を実行するキャッシュ機構２２とを含んでいる。

明細書

Webサービス提供システム、そのためのサーバ装置、コンピュータ・システムをWebサービス提供システムのためのサーバ装置として制御するための制御方法、および該制御方法を実行するためのプログラムおよび記録媒体

技術分野

本発明は、効率的なWebサービスの提供に関し、より詳細には、ユーザが過去に閲覧したWebサービスの情報に基づき、高速、かつ高信頼性をもってユーザに対してWebサービスの提供を可能とすると共に、ユーザのアクセス権限の変更およびWebサービス提供者のWebサービスへのアクセス権限変更に対して高い柔軟性を付与することが可能なWebサービス提供システム、そのためのサーバ装置、コンピュータ・システムをWebサービス提供のためのサーバ装置として制御するための制御方法、および該制御方法を実行するためのプログラムおよび記録媒体に関する。

背景技術

単純にWebページを表示させるといったスタティックなコンテンツから、JSP（Java（登録商標） Service Provider）のようなダイナミックなコンテンツにいたるまで、様々なコンテンツに対応したWebサービスのためのキャッシュ機構が知られている。例えばWebサービスを行うためのキャッシュ機構として、WebSphereのDynaキャッシュを挙げることができる。従来知られているキャッシュ機構は、以前に実行した結果を覚えておき、ユーザがWebサービスに再度アクセスする際に、実際にサービス・オブジェクトを実行するのではなく、キャッシュ機構に記憶させておいた過去の実行結果を返すことで応答性能を向上させている。

一方で、Web上でサービスを提供する場合には多くの場合、ユーザに応じてアクセスを制限できるようにすることが好ましい場合もあり、ユーザのアクセス権限に応じてアクセスを制限するためのアクセス制御機構も知られている。より具体的には例えば、銀行のATMサービスを提供するWebサイトを構築する場合、ユーザには、その信用や長期預金額などにより、Gold会員、Silver会員、Bronze会員のクラス分け（以下、アクセス権限として参照する。）を付与して高い付加価値のサービスを用意することができる。この場合、Bronze会員は、一般の顧客であり、クラスがSilver、Goldとグレードが高くなるにつれて、ユーザは、より高い価値のサービスの提供を受ける。上述したWebサービスとしては、通常の預金操作の他、アクセス権限で差別化された株（天気）情報の提供、エンターテイメント情報、不動産情報も考えられる。

上述したユーザのアクセス権限に応じたWebサービスの提供における上述したアクセス制限機能としては、具体的にはHTTPのBasic Authや、EJBにおけるアクセス権限に基づくメソッド単位のアクセス制御機構を挙げることができる。

図２１には、従来のアクセス制御機構を含むWebサービス提供システムの概略的な処理を示す。図２１が従来のアクセス制御機構の処理を示した概略図である。図２１に示したWebサービス提供システムのアクセス制御機構は、Webサービスを提供するサーバ装置１０２に備えられており、ユーザは、コンピュータ、セルラ電話、ＰＤＡといったユーザ端末１０４からサーバ装置１０２へと、有線ネットワークや、無線ネットワーク、またはこれらが混在した複合ネットワークであるネットワーク１０６を

介してサーバ装置１０２へとアクセスしている。サーバ装置１０２へのアクセス認証は、通常ではユーザ識別を実行するためのコード（以下、ユーザＩＤとして参照する。）およびパスワードといった公衆鍵と秘密鍵との組み合わせにより行われる。サーバ装置１０２によりユーザ認証がなされると、ユーザにより送られたアプリケーション要求、例えば天気予報の情報の提供を行うWeatherというアプリケーションの呼出しを要求するオブジェクト呼出し要求がサーバ装置１０２へと入力される。

アプリケーションWeatherは、さらにユーザのアクセス権限に応じて、大まかな天気予報をユーザに提供するためのメソッドであるRoughWF()、より多様で高付加価値の情報を提供することができるメソッドであるWeatherForecast()などを呼出すことが可能とされている。ユーザには、例えばサービス提供者との契約などに基づき、上述したGold、Silver、Bronzeといったアクセス権限が付与されている。図２１に示した従来例では、Silverのアクセス権限を有するユーザが、ユーザ端末１０４からサーバ装置１０２へとアクセスしているのが示されている。ユーザは、Weather getRoughWF ()といったSilverのユーザにアクセス権限に対応した実行結果を取得し、実行結果は、ブラウザ・ソフトウエアを使用してユーザへとデータが提供される。

また、Goldユーザは、Weatherのアプリケーションにおいてさらに、別のgetWeatherForecast ()というメソッド呼出しが許可されており、さらにその中で、getDetailedInfo というメソッドを呼出すこが許可されているなど、より高い価値のWebサービスへのアクセスが許可される。図２１では、Goldのアクセス権限を有するユーザのみがメソッドgetDetailedInfo ()のデータを取得することができ、Silverのアクセス権限を有す

るユーザは、例えば、getDetailedInfo()のメソッドの実行結果を受け取ることができないことが示されている。

図２１に示すように、Webサービス提供に対応するメソッドgetRoughWF()およびgetWeatherForecast()については、GoldまたはSilverのアクセス権限を有するユーザに対してアクセスが許されているものとする。このとき注意しなければならないのは、最初に呼ばれるメソッドへのアクセスが許されている場合でも、そのメソッドの内部でさらに呼出されるメソッドへのアクセスが許されているとは限らないことにある。図２１のgetWeatherForecast()は、その例であり、メソッドgetWeatherForecast()の内部で呼ばれているメソッドgetDetailedInfo()は、アクセス権限がSilverであるユーザには、アクセスが許されていない。このため、実行結果を返す場合に、getDetailedInfo()が呼出される場合には、メソッドgetWeatherForecast()の実行結果を、アクセス権限がSilverのユーザに返してはならない。一方、メソッドgetRoughWF()は、その後Silverのアクセス権限を有するユーザによるアクセスが許されていないメソッドが呼ばれていないので、その実行結果をSilverのアクセス権限のユーザに返すことができる。

図２２は、図２１に示した従来のアクセス制御機構における他の不都合を示した図である。図２２では図２１と同様に、ユーザは、ユーザ端末１０４からサーバ装置１０２へとネットワーク１０６を介してアクセスする。図２６では、サーバ装置１０２が含むアクセス制御機能１０８が示されており、アクセス制御機能１０８によりアクセス権限がSilverのユーザが、例えばアクセス権限がGoldのユーザにのみ許可される要求がサーバ装置１０２に入力された場合には、その要求を実行させないこ

とで、アクセス権限がSilverであるユーザが不正にGoldのアクセス権限を必要とするサービスにアクセスしてしまうことを防止している。

一方で、Silverのアクセス権限を有するユーザは、アクセス権限がSilverのユーザに許可されるWeather getRoughWF ()により与えられる実行結果を取得することができる。アクセス権限がSilverのユーザは、許可されたデータの取得が可能ではあるものの、サーバ装置１０２は、アクセス制御を要求されたメソッドを呼出すたびに実行させる必要があるので、データをブラウザ・ソフトウエア上に表示させるまで長時間を要するといった時間遅延を生じることになる。このような不都合は、サーバ装置の能力や、処理の複雑さなどに依存するので、ADSL、光通信といったブロードバンド通信が普及し、サーバ装置－ユーザ端末間の通信速度が高くなっても改善されるものではない。

上述した従来の不都合を改善するために、サーバ装置１０２にキャッシュ機構を導入することもできる。図２３は、従来のアクセス制御機構に対して、キャッシュ機構を導入したシステムを示す。

図２３に示したシステムは、サーバ装置１０２がキャッシュ機構１１０を含んで構成されており、ユーザが送信したオブジェクト呼出し要求により呼出されたオブジェクトが実行した実行結果が、キャッシュ機構１１０に格納される構成とされている。図２３に示されるように、サーバ装置１０２に対してキャッシュ機構１１０とアクセス制御機構１０８とを構成させる場合には、ユーザはそれぞれのアクセス権限を有するサービスに対して適正なアクセス権限を行使して実行結果を取得することが可能となる。またユーザにより取得された実行結果は、キャッシュ機

構１１０に格納されるので、過去に要求したと同一のオブジェクト呼出を要求するユーザは、キャッシュ機構に格納された過去の実行結果を容易に取得することが可能となる。また、キャッシュ機構から送られた実行結果に基づいてその後の処理を容易に実行させることが可能となる。しかしながら、従来のアクセス制御を伴うWebサービスに関していえば、後述する理由から、キャッシュ機構を使用しない構成が採用されてきた。

すなわち、図２３に示されるように、サーバ装置１０２に対してキャッシュ機構１１０と、アクセス制御機構１０８とを同時に使用する場合を考える。キャッシュ機構１１０が、ユーザのアクセス権限に無関係にユーザのアクセスを許可してしまう場合には、いったんキャッシュ機構に格納された実行結果が、ユーザのアクセス権限に関係なく同一のサービスを要求するユーザに対して提供されてしまうという不都合が生じる。このようなアクセス権限に基づかないキャッシュ機構へのアクセスが許可されると、Webサービスへのアクセス制御をしているにもかかわらず、キャッシュ機構を設けたことにより、アクセス権限のクラスに応じて提供される高付加価値情報や、ユーザへの特典がキャッシュ機構を介してアクセス権限のないユーザに対して提供されることになり、高付加価値のWebサービスの有効性やサービスへの誘因提供性が失われてしまうことにもなる。

このため、キャッシュ機構へのアクセスについてもユーザのアクセス権限に関連して制御する必要が生じることになる。この場合ユーザからのオブジェクト呼出し要求ごとに呼出されるメソッドへのアクセス権限をその度ごとに判断し、キャッシュ機構へのアクセス制御とWebサービス

へのアクセス制御とを同時に実行させるのでは、処理に時間がかかり、キャッシュ機構を設けることによりユーザへの実行結果の表示を高速化するという点では著しい不都合を与えることになる。また、ユーザのアクセス権限が変更されたり、サービス提供者のアクセス条件が変更された場合に、キャッシュ機構へのアクセスにより生じる高付加価値情報のリークに容易に対応することができることが好ましい。このため、ユーザへのWebサービス提供性能の向上という観点からいえば、アクセス制御とキャッシュ機構とを同時に使用して、高い信頼性の下で、可能な限りWebサービスを提供することが望まれていた。

本発明は上記従来技術の不都合に鑑みてなされたものであり、本発明は、高い信頼性で、高付加価値のWebサービスを可能な限り迅速に提供することを可能とするWebサービス提供システムを提供することを目的とする。さらに本発明は、コンピュータ・システムを上述したWebサービスを提供することができるサーバ装置装置を提供することを目的とする。さらに本発明は、コンピュータ・システムを上述したサーバ装置装置として機能させることが可能なサーバ装置制御方法を提供することを目的とする。また本発明のさらに別の目的は、コンピュータ・システムを上述したサーバ装置装置として機能させるためのプログラム、および該プログラムを記録したコンピュータ可読な記録媒体を提供することを目的とする。

発明の開示

本発明は、Webサービスが許可するオブジェクトをあらかじめ解析しておき、オブジェクトが呼び出すメソッドのアクセス権限を取得してアク

セス権限セットを生成しておく。その後、オブジェクトとアクセス権限セットとを対応させておくことにより、所定のアクセス権限が付与されたユーザがWebサービスを要求した場合に、ユーザの要求する要求オブジェクトに対応するアクセス権限セットと、ユーザのアクセス権限とから、キャッシュ機構へのアクセスを許可する機能をサーバ装置装置に付与することができれば、Webサービスの高速性および高信頼性を提供することが可能となる、という着想の下になされたものである。

本発明では、上記機能を達成するためにあらかじめJava（登録商標）のコードを解析しておき、所定のサービスの実行を完遂するのに呼び出される可能性のあるメソッドをすべて列挙する。一方で、列挙されたメソッドすべてのアクセス権限をリストして、オブジェクトに対するアクセス権限セットのリスト（以下、オブジェクトーアクセス権限リストとして参照する。）をあらかじめ生成し、格納しておく。このリストを使用して要求オブジェクトに対するWebサービスを要求したユーザのアクセス権限を判断し、リストにより許可されるユーザにのみキャッシュ機構に対するアクセスを許可し、実行結果（以下、キャッシュ・エントリとして参照する。）として格納された過去に実行されたオブジェクトの実行結果を返す。本発明のサーバ装置装置によれば、キャッシュ機構が本来的に許可されないメソッドの実行結果に対応するキャッシュ・エントリの値を、ユーザに対して返してしまうことはない。また、キャッシュされた過去の実行結果が得られない場合には、キャッシュ機構は、ユーザからのオブジェクト呼出し要求をオブジェクトの実行部に渡し、その実行結果をアクセス権限の範囲内でユーザに取得させることが可能となる。

本発明では、上記の機能をサーバ装置装置に対して付与するために、Webサービスを実行させるオブジェクトを解析し、呼び出される可能性のあるメソッドに対応したアクセス権限を取得することで、オブジェクトの実行に必要なアクセス権限セットを抽出する手段を提供する。生成されたアクセス権限セットは、オブジェクトごとに対応づけられたリストとして格納され、ユーザがキャッシュ・エントリにアクセス可能かどうかを判定するために読出され、キャッシュ・エントリに対するユーザのアクセス可否が決定される。

上述したオブジェクト解析では、必要なアクセス権限を抽出する、具体的には、EJBのようなコードと設定ファイルとがパッケージ化されたオブジェクト・プログラムを対象として、所定のオブジェクトを呼出す際に呼出されるすべてのメソッドが特定される。ついで、それらのメソッドに与えられたアクセス権限を集めてアクセス権限セットのリストを構成させる処理を実行する。本発明によれば、アプリケーションに応じて呼出しが行われる可能性のあるすべてのメソッドに対するアクセス権限を保有するユーザに対してのみ、キャッシュ・エントリへのアクセスが許可され、高信頼性を提供することができる。

さらに本発明では、キャッシュ機構とオブジェクト解析機構とが完全に独立しているので、解析された情報に基づいて、管理者の責任においてキャッシュ機構に条件を緩めて必要なユーザ権限を設定することも可能であるし、さらには、ユーザのアクセス権限のアップグレードや、ダウングレードに伴う変更に対しても、ユーザの変更後のアクセス権限を変更するだけで、キャッシュ機構へのアクセス機構に対してなんらの付加的な機構を設けることなく、高速、かつ高信頼性のWebサービスを提供

することが可能となる。

すなわち、本発明によれば、ネットワークを介してWebサービスを提供するためのサーバ装置を含むWebサービス提供システムであって、前記サーバ装置は、

前記ネットワークを介して受信したオブジェクト呼出し要求と、ユーザ識別子とを取得すると共に、取得したオブジェクト呼出し要求を格納させ、かつ前記ユーザ識別子により指定されるアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、

過去に実行されたオブジェクトの実行結果を格納する記憶部と

を含み、前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、Webサービス提供システムが提供される。

本発明では、前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させることができる。また、本発明では、前記サーバ装置はさらに、オブジェクト実行手段を含み、前記制御手段は、前記記憶部に該当する過去の実行結果が格納されていない場合に、前記オブジェクト呼出し要求をオブジェクト実行部に送り前記要求オブジェクトを実行させることができる。本発明においては、前記サーバ装置は、前記制御手段を含むエッジ・サーバと、前記オブジェクト実行部を含むアプリケーション・サーバとから構成されていてもよい。

本発明によれば、ネットワークを介してWebサービスを提供するためのサーバ装置であって、前記サーバ装置は、

オブジェクト呼出し要求を受取り、かつ格納させると共に、要求オブジェクトへのアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、

過去に実行されたオブジェクトの実行結果を格納する記憶部と

を含み、

前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、サーバ装置が提供される。本発明では、前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させることができる。

さらに、本発明によれば、ネットワークを介してWebサービスを提供するためのサーバ装置であって、前記サーバ装置は、

要求オブジェクトが呼出す可能性のあるメソッドすべてを取得してアクセス権限セットを生成するオブジェクト・アナライザ手段と、

前記要求オブジェクトを実行するためのオブジェクト実行手段と、

過去のオブジェクトの実行結果を格納する記憶部を含んで構成され、かつ前記アクセス権限セットを使用して前記オブジェクト呼出し要求に応答して前記記憶部に対するアクセス制御を実行するキャッシュ機構と

を含むサーバ装置が提供される。

本発明における前記キャッシュ機構は、

要求管理部と、

前記記憶部に格納された過去の要求オブジェクトの実行結果の検索を制御するアクセス制御部とを含んで構成することができる。本発明では、前記アクセス制御部は、前記要求オブジェクトに対するアクセス権限と、前記アクセス権限セットとを比較してアクセス制御を実行し、

前記要求管理部は、前記アクセス制御部の判断に応答して前記オブジェクト呼出し要求を前記オブジェクト実行部へと渡して前記要求オブジェクトの実行を制御することができる。本発明では、前記オブジェクト・アナライザ手段は、さらにオブジェクトのコードから前記オブジェクトが呼出す可能性のあるメソッドを取得する手段と、該メソッドに対応するアクセス権限を取得する手段と、前記オブジェクトが呼び出す可能性のあるすべてのメソッドへのアクセス権限から前記アクセス権限セットを生成して格納させる手段とを含むことができる。

本発明によれば、コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのサーバ制御方法であって、前記方法は、前記コンピュータ・システムに対して、

オブジェクト呼出し要求を受信し格納するステップと、

要求オブジェクトへのアクセス権限をメモリから取得するステップと、

前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、

前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記要求オブジェクトの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップと

を実行させる、サーバ制御方法が提供される。

また、本発明では、前記記憶部が過去に実行された要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信するステップを実行させることができる。さらに本発明では、前記記憶部が過去に実行された要求オブジェクトの実行結果を格納しない場合には、前記オブジェクト呼出し要求をオブジェクト実行部へと渡すステップを実行させることができる。

本発明によれば、コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、

オブジェクト呼出し要求を受信し格納するステップと、

要求オブジェクトへのアクセス権限をメモリから取得するステップと、

前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、

前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納し

た記憶部を検索させるステップと

を実行させる、プログラムが提供される。

また、本発明によれば、コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対して、

オブジェクト呼出し要求を受信し格納するステップと、

要求オブジェクトへのアクセス権限をメモリから取得するステップと、

前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、

前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップと

を実行させる、コンピュータ可読な記憶媒体が提供される。

本発明によれば、コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、

要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、

前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップと

を実行させるプログラムが提供される。

また、本発明によれば、コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対して、

要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、

前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップと

を実行させる記憶媒体が提供できる。

図面の簡単な説明

図１は、本発明のWebサービス提供システムの概略的な構成を示した図。

図２は、本発明のサーバ装置装置の機能ブロックを示した図。

図３は、本発明のオブジェクト・アナライザの機能ブロックを示した図。

図４は、本発明のキャッシュ機構における処理を示したフローチャート。

図５は、本発明のキャッシュ機構におけるキャッシュ・エントリが見出されなかった場合の処理を示したフローチャート。

図６は、本発明におけるユーザーアクセス権限テーブルの実施の形態を示した図。

図７は、本発明におけるオブジェクトーアクセス権限リストの実施の形態を示した図。

図８は、本発明のメソッドーアクセス権限テーブルの実施の形態を示した図。

図９は、本発明におけるキャッシュ・エントリの構成を示した図。

図１０は、本発明におけるアクセス権限セット生成処理を示した概略図。

図１１は、本発明におけるオブジェクト・アナライザにおける処理を示したフローチャート。

図１２は、本発明におけるオブジェクト・アナライザにおける処理を示したフローチャート。

図１３は、図１１および図１２に示したオブジェクト・アナライザにおける本質的な処理部分の擬似コードの実施の形態を示した図。

図１４は、本発明のオブジェクト・コード解析の他の実施の形態を示した概略図。

図１５は、本発明のアクセス権限判断を実行させる処理のフローチャート。

図１６は、図１５に示したアクセス権限判断を実行させるための擬似コードの実施の形態を示した図。

図１７は、本発明のWebサービス提供システムのトランザクションの実施の形態を示した図。

図１８は、本発明のWebサービス提供システムのトランザクションの実施の形態を示した図。

図１９は、本発明のWebサービス提供システムのトランザクションの実施の形態を示した図。

図２０は、本発明のサーバ装置装置の他の実施の形態を示した図。

図２１は、従来のアクセス制御機構を含むWebサービス提供システムの処理を示した図。

図２２は、従来のアクセス制御機構を含むWebサービス提供システムの処理を示した図。

図２３は、従来のアクセス制御機構とキャッシュ機構とを含むWebサービス提供システムの処理を示した図。

発明を実施するための最良の態様

以下、本発明を図面に示した具体的な実施の形態に基づいて説明するが、本発明は、後述する実施の形態に限定されるものではない。

Ａ：Webサービス提供システムの概略構成

図１は、本発明のWebサービス提供システムの概略的な構成を示した図である。図１に示したWebサービス提供システム１０は、ユーザ端末１２と、サーバ装置１４と、ユーザ端末１２と、サーバ装置１４との間を遠隔的に接続するネットワーク１６とを含んで構成されている。本発明において使用することができるユーザ端末１２としては、デスクトップ・コンピュータ、ノート型コンピュータ、携帯型コンピュータといったコンピュータの他、セルラ電話などを挙げることができる。また、本発明において使用することができるサーバ装置１４としては、パーソナル・コンピュータ、ワークステーションといったコンピュータ・システムを使用することができる。ユーザ端末１２と、サーバ装置１４とを接続するためのネットワーク１６としては、ＴＣＰ／ＩＰなど、これまで知られたいかなる通信プロトコルを使用するネットワークであっても使用でき、ＩＳＤＮ、ＡＤＳＬといった通信回線、無線ネットワーク、地上波通信、衛星通信、およびこれらを任意に組み合わせ、サーバ装置１４へ

のアクセスを可能とする限り、いかなるものでも使用することができる。

ユーザは、図１に示したWebサービス提供システムにおいて、サーバ装置１４から高付加価値のサービスの提供を受けるため、サービス提供者などと契約して、ユーザＩＤ、パスワードといった認証情報を取得している。ユーザは、Webサービス提供システムにアクセスする場合には、インターネットといったネットワーク１６にアクセスし、ＵＲＬアドレスなどを指定してユーザ識別子であるユーザＩＤ、パスワードなどを入力する。サーバ装置１４は、アクセス認証の後、特定のＵＲＬサイトにおけるWebサービスを許可する構成とされている。

本発明における高付加価値のサービスとは、種々のサービスを挙げることができるが、例えばユーザのクラス分け（以下、アクセス権限：roleとして参照する。）に応じて、順次詳細な情報を提供することができる天気予報サービス、ユーザのクラス分けに応じて金利やメリットが変化する金融サービス、株式情報サービス、医療サービス、エンターテイメント提供サービスなどを挙げることができる。

以下、本発明を具体的に説明するために、Webサービス提供システムは、Servlet/EJB/DBを用いた標準的な3 tier構成であるものとし、EJB部分は、ユーザごとに作られるセッション・ビーンと、各セッションから共通して使われるエンティティ・ビーンからなるものとする。株または天気情報は、特定の実施の形態として、セッション・ビーン、getStockRecommendation()、getWeatherForecast()により提供されており、データベースと結びついている株（天気）エンティティ・ビーンgetStockInfo()、g

etDetailedInfo()を呼出してその情報を構築するものとする。

本発明では、ユーザ単位に構成されるためアクセス制御のいらないセッション・ビーンではなく、エンティティ・ビーンの各メソッドにはアクセス権限ベースでのアクセス制御が実行されるものとする。セッション・ビーンによりユーザ認証が実行され処理が進行するものとする。

なお、以下の実施の形態で説明する各メソッドと、アクセス権限との関係は、getDetailedInfo()はGoldのみ、getDetailedStock()はSilverとGoldのみがアクセスできるものとする。また、getWeatherForecast()は、アクセス権限に応じて、Bronze/Silverの場合は、おおまかな天気予報を返すが、Goldの場合は正確な天気予報を返すものとする。さらに、getStockRecommendation()は、アクセス権限に応じて、Bronzeのアクセス権限では、場合は単純な株情報を返すが、SilverとGoldのアクセス権限に対してはgetDetailedStock()を呼出して高度なおすすめ株情報を返すメソッドであるものとする。

サーバ装置１４へのアクセスが認証されたユーザは、その後、要求するWebサービスを実行するためのオブジェクト呼出し要求をサーバ装置１４へと送る。サーバ装置１４は、オブジェクト呼出し要求から要求オブジェクトを特定し、サービスの提供を行なっている。Webサービスに必要とされる情報は、データベース１８に格納されていて、要求オブジェクトにより検索や、処理が実行され、ユーザへと提示される構成とされている。本発明のサーバ装置１４は、ユーザに付与されたアクセス権限に基づく要求オブジェクトへのアクセス制御を実行していると共に、ユーザが過去にアクセスしたオブジェクトの実行結果を記憶するキャッシュ

機構を含んで構成されている。このキャッシュ機構は、ユーザが過去にアクセスしたと同一のサービスを同一のアクセス権限、または本発明の他の実施の形態ではより高いクラスのアクセス権限で要求した場合には、キャッシュ機構にキャッシュ・エントリとして格納された実行結果へのアクセスが許可される。キャッシュ機構へとアクセスして実行結果の値をユーザに返すまでの処理は、アプリケーションを実際に実行するよりも本発明においては高速である。

このため、キャッシュ機構に格納された実行結果を取得することで、最初に同一のWebサービス提供を要求した場合に比較して、より高速のデータ提供が可能とされている。また、ユーザが初めて要求するオブジェクトの場合には、キャッシュ・エントリを参照しても該当するキャッシュ・エントリがないのでサーバ装置１４において、Webサービスを提供するためのオブジェクトが呼び出され、アクセス権限に対応して各メソッドが実行される。サーバ装置１４は、実行結果をユーザに返すことによりユーザに対してWebサービスを提供すると共に、実行結果をキャッシュ機構の新たなエントリとして追加して格納する。

図２は、本発明のサーバ装置１４の概略的な機能ブロックを示した図である。図２に示すように、本発明のサーバ装置１４は、ネットワーク１６を介して送受信を行うための送受信部２０と、キャッシュ機構２２と、Webサービスを提供するためのオブジェクトを解析してオブジェクトが呼出す可能性のあるメソッドのアクセス権限セットを、メソッドごとのアクセス権限に基づいて生成するオブジェクト・アナライザ２４と、Webサービスのためのオブジェクト呼出して実行するためのオブジェクト実行部２６とを含んで構成されている。キャッシュ機構２２は、受信し

たオブジェクト呼出し要求とユーザに与えられた所与のアクセス権限とアクセス権限セットとに基づいて、キャッシュ機構２２に格納されたキャッシュ・エントリの検索を可能とさせている。

オブジェクト・アナライザ２４は、本発明の特定の実施の形態では、オブジェクト実行部２６が使用するEJBといったオブジェクトのコードを解析し、コード上で呼出しが行われる可能性のあるメソッドを取得する。この解析は、EJBにおける構文を解析して、呼びされるメソッドをたとえば、ハッシュ・テーブルに格納するなどにより実行される。その後、取得したメソッドに対応するアクセス権限を、メソッドに割当てられたアクセス権限をリストした、メソッドーアクセス権限テーブルをルックアップして取得し、オブジェクトを実行させるためのアクセス権限をすべて取得する。すべてのアクセス権限を取得した後、オブジェクト・アナライザ２４は、オブジェクトーアクセス権限リストを生成し、生成されたアプリケーションーアクセス権限リストは、例えば適切なメモリ３８に登録される。

オブジェクト実行部２６は、ハードディスクといった記憶手段２８に格納されたオブジェクトを適切なメモリに呼出して実行させ、ユーザから要求されたオブジェクトに対する実行結果を生成し、生成した実行結果をメモリ３８に渡している。キャッシュ機構２２は、メモリ３８から実行結果を読出して、要求オブジェクトの実行結果をユーザに提供すると共に、新たなキャッシュ・エントリとして格納させ、将来のユーザ要求に対して高速なWebサービスの提供を可能とさせている。

図２に示したキャッシュ機構２２は、さらに詳細には要求管理部３０

と、アクセス制御部３２と、記憶部３４とを含んで構成されている。図２に示されたキャッシュ機構２２は、要求管理部３０と、アクセス制御部３２とがサーバ装置１４内に配置されていて、記憶部３４への制御手段を構成している。また、図２では、記憶部３４は、図面上ではサーバ装置１４の外部に配置されているものの、サーバ装置１４における内蔵ハードディスクなどを使用することができる。要求管理部３０は、ユーザから送られたユーザＩＤをキーとして、ユーザーアクセス権限テーブルをルックアップし、ユーザに与えられた所与のアクセス権限を取得する。また、ユーザが送信するオブジェクト呼出し要求のデータから、ユーザが希望するサービスを実行するオブジェクトを特定し、特定されたオブジェクトを一義的に指定するため、例えばオブジェクト呼出し要求をテキスト・コードとし、当該テキスト・コードを識別子として使用することができる。以下、本発明においてはオブジェクト識別子として、オブジェクト名を使用するものとして説明を行うが、本発明においては他のいかなる識別手法を使用することもできる。オブジェクト名は、その後アクセス制御部３２へと渡される。アクセス制御部３２は、ユーザが保有するアクセス権限を、メモリ３８に格納されたオブジェクトーアクセス権限リストを読出して比較を行い、ユーザが保有するアクセス権限が、ユーザが要求された要求オブジェクトに該当するか否かを判断する。

ユーザが要求した要求オブジェクトがユーザのアクセス権限で使用が認められる場合には、アクセス制御部３２は、ユーザが要求したオブジェクト名に対応するキャッシュ・エントリ３６を検索させる。該当するキャッシュ・エントリ３６ａが見出された場合には、キャッシュ・エントリ３６ａの値をアクセス制御部３２へと渡して、ユーザへと実行結果

として提供し、さらに後続するユーザからの要求に対応する。また、ユーザが錯誤または意図的にアクセス権限のないオブジェクトの要求を行った場合には、アクセス制御部３２は、ユーザのアクセス権限を、オブジェクトーアクセス権限リストと比較して、正当なアクセス権限がないものと判断し、要求管理部３０に対してアクセスを許可しない通知を行う。この通史は、アクセス不可フラグを送信するなど、これまで知られたいかなる方法でも使用することができる。

また、本発明の他の実施の形態では、ブラウザ・ソフトウエアを介して、ユーザに、アクセス権限がないのでWebサービスにアクセスできないことを表示することもできる。また、ユーザが適切なアクセス権限を保有しているが記憶部３４に該当するキャッシュ・エントリが見出されない場合には、要求管理部３０へとキャッシュ・エントリなしの通知が送られる。要求管理部３０は、その通知を受け取ると、適切なメモリ、例えばメモリ３８に一時的に格納しておいたユーザが要求したオブジェクト呼出し要求を、オブジェクト実行部２６へと渡す。オブジェクト実行部２６は、オブジェクトを呼出して実行させ、ユーザが要求した実行結果を生成する。生成された実行結果は、メモリ３８へと格納される。要求管理部３０は、格納された実行結果を読出し、Netscape Navigator（商標）や、Internet Explorer（商標）といったブラウザ・ソフトウエアを使用して、ユーザに対して提供することができる構成とされている。

図３は、本発明のオブジェクト・アナライザ２４の概略構成を示した図である。本発明におけるオブジェクト・アナライザ２４は、入力バッファ４０と、パーサ４２と、メソッドーアクセス権限テーブル４４と、アクセス権限セット生成部４６とを含んで構成されている。オブジェク

ト・アナライザ２４は、入力バッファ４０にオブジェクト実行部２６が使用するオブジェクトを記憶手段２８からあらかじめ取得させ、入力バッファ４０に格納されたオブジェクトを、パーサ４２へと渡して、オブジェクトのコードを解析させる。解析の結果、オブジェクトに呼出される可能性のあるメソッドが取得されると、メソッドを適切なメモリに格納する。

オブジェクト・アナライザ２４は、メモリからメソッドを読出して、メソッドーアクセス権限テーブル４４をルックアップし、当該メソッドに対して、Webサービス提供者により指定されたアクセス権限を取得し、アクセス権限セット生成部４６に渡す。アクセス権限セット生成部４６は、渡されたメソッドごとのアクセス権限を使用して、所定のオブジェクトに対応するアクセス権限セットを生成する。生成されたアクセス権限セットは、出力バッファ４８へと一時的に格納される。オブジェクト・アナライザ２４は、出力バッファ４８に蓄積されたアクセス権限セットを、メモリ３８へとオブジェクト名と対応させて格納させることにより、オブジェクトーアクセス権限リストを生成させる。

本発明においては、上述したオブジェクト・アナライザ２４を設け、オブジェクトの呼出しにより呼出される可能性のあるメソッドとアクセス権限とをあらかじめ取得しておき、オブジェクトーアクセス権限リストとして適切なメモリ、例えばメモリ３８に登録する。このため、Webサービスを提供するオブジェクトが新たに追加されるまでオブジェクトーアクセス権限リストの再構築をする必要がなく、高速のアクセス判断を可能とする。また、さ新たにWebサービスに対応するオブジェクトが追加された場合でも、実際にオブジェクトがユーザにより要求される前に解

析しておくことが可能なので、オブジェクト・プログラムの追加があった場合にでも、最小のコストで、高速かつ高信頼性のWebサービスを提供することが可能となる。

B：本発明のキャッシュ機構の実行する処理

図４は、本発明におけるキャッシュ機構の処理のフローチャートを示した図である。本発明におけるキャッシュ機構の処理は、ステップＳ１０においてユーザからのオブジェクト呼出し要求を受信して、要求オブジェクト名を特定する。次いで、取得された要求オブジェクト名は、ステップＳ１２において適切なメモリに格納される。ステップＳ１４では、先だって送られた、またはオブジェクト呼出し要求と共に送られたユーザＩＤをキーとして、ユーザーアクセス権限テーブルをルックアップさせることでユーザに与えられたアクセス権限を取得し、メモリに登録する。ステップＳ１６では、取得されたユーザのアクセス権限と、オブジェクト名とを使用して、オブジェクトーアクセス権限リストのエントリをメモリから読み出し、比較する。

ステップＳ１６における比較の結果、要求されたオブジェクトがユーザのアクセス権限で実行可能な場合（yes）には、ステップＳ１８に進む。ステップＳ１８では、オブジェクト名を検索キーとして使用して記憶部３４に格納されたキャッシュ・エントリの検索を実行させる。ステップＳ１８で、キャッシュ・エントリが見出された場合(yes)には、ステップＳ２０において、キャッシュ・エントリが見出されたことをアクセス制御部に通知する。ステップＳ２２では、検索された実行結果を受け取ったアクセス制御部は、要求処理部へと通知して、キャッシュ・エントリの値を取得させ、ブラウザ・ソフトウエアを使用してユーザに提示して、

Webサービスの提供を可能とする。

また、ステップＳ１６においてユーザのアクセス権限がオブジェクトーアクセス権限リストにより記憶部３４へのアクセス可ではないと判断された場合(no)には、ステップＳ２４でアクセス制御部にアクセスが拒否されたことが通知される。また、本発明の説明している実施の形態では、ステップＳ２６において要求処理部からユーザへとアクセスが拒否されたことが通知されている。同時に、要求差オブジェクト呼出し要求は、キャッシュ機構内から廃棄される。

図５は、図４のステップＳ１８でキャッシュ・エントリが見出されなかった場合(no)の詳細な処理を示した図である。ステップＳ１８でキャッシュ・エントリが見出されなかった場合(no)には、ステップＳ２８でアクセス制御部に通知を行い、ステップＳ３０において適切なバッファ・メモリに格納しておいたオブジェクト呼出し要求をオブジェクト実行部へと渡す。オブジェクト呼出し要求を受け取ったオブジェクト実行部は、要求オブジェクトを呼出して実行させ、実行結果を適切なメモリ、例えばメモリ３８に格納する。ステップＳ３２において要求処理部は、実行結果をメモリ３８から読出し、ステップＳ３４で実行結果をブラウザ・ソフトウエアを使用してユーザに提供する。また、ステップＳ３６では、実行結果がオブジェクト名とアクセス権限セットとが適切なメモリ領域から読出され、ステップＳ３８でオブジェクト名と、アクセス権限セットと、実行結果とが記憶部における新たなキャッシュ・エントリとして登録される。

Ｃ：キャッシュ機構が使用するデータ構成

図６は、本発明のアクセス制御部３２が使用するユーザーアクセス権限テーブルのデータ構成を示した図である。ユーザーアクセス権限テーブルは、図６に示すように、ユーザを特定するためのユーザＩＤと、それに対応するアクセス権限(Gold、Silver、Bronze)とが対として構成されている。このテーブルは、Webサービスを提供する者またはサーバ装置管理者により入力され、例えば、ハードディスク２８、ユーザ・データベースなどに格納しておくことができる。図６に示したユーザーアクセス権限テーブルは、例えばサーバ装置装置１４が管理する図示しないユーザ・データベースに格納しておくことができる。サーバ装置１４がユーザからのユーザＩＤを受信すると、ユーザＩＤが適切なメモリに格納され、格納されたユーザＩＤは、アクセス制御部３２により読出され、読み出されたユーザＩＤをキーとしてユーザーアクセス権限テーブルをルックアップすることにより、ユーザのアクセス権限がアクセス制御部３２により取得される。

図７は、アクセス制御部３２が使用するオブジェクトーアクセス権限リストの実施の形態を示した図である。図７では、アクセス権限が、Gold、Silver、Bronzeで示されており、それぞれのオブジェクト１およびオブジェクト２に対するアクセス権限がyesまたはnoで示されている。オブジェクトとしては具体的には上述した天気予報では、getWeatherForecast()とすることができ、株式情報では、getStockRecommendation()とすることができる。オブジェクト１に対してBronzeのアクセス権限に対してyesのアクセス権限を生成するためには、呼出される可能性のあるメソッド１、メソッド２、メソッドｚがすべてBronzeのアクセス権限のユーザに対してアクセスできることが必要となる。

アクセス制御部３２は、ユーザから送られたユーザＩＤに基づき、図６に示したユーザのアクセス権限、Gold、Silver、Bronzeを取得した後、オブジェクト識別子をキーとして使用して、図７に示したオブジェクトーアクセス権限リストをルックアップする。その後、オブジェクトと要求されたメソッドとをルックアップして比較を行い、呼び出されるメソッドのうちの１つでもアクセス権限がnoとなる場合には、アクセス許可フラグを設定しないなどにより、記憶部３４へのキャッシュ・アクセスを実行させない。なお、「キャッシュ・アクセス可」は、記憶部３４を参照できると共に、新たなデータを記憶部３４に書込むことができることを意味する。また、アクセス権限セットは、図７に示した１つのアプリケーションに対する縦方向のコラムが、アクセス権限セットの具体的な要素を示している。

図８は、本発明のオブジェクト・アナライザ２４が使用することができる、メソッドーアクセス権限テーブルの実施の形態を示す。メソッドーアクセス権限テーブルは、オブジェクトが呼び出す可能性のあるメソッドと、当該メソッドを実行することができるアクセス権限、例えばGold、Silver、Bronzeとが対として登録されたテーブルとして構成することができる。このテーブルは、サービス提供者やサーバ装置管理者などにより作成され、例えば、データベース２８や、ユーザ・データベースなどに格納することができる。

図９は、記憶部３４が格納するキャッシュ・エントリの具体的な構成を示した図である。図９に示されるように、記憶部３４は、過去にアクセスされたWebサービスを実行させるためのオブジェクト名と、アクセス権限セットと、対応するオブジェクトの実行結果とがキャッシュ・エン

トリ３６を構成している。オブジェクト呼出し要求を受信して、キャッシュ・アクセス可と判定されたユーザ要求は、アクセス制御部３２により、オブジェクトを実行するに先立って対応するオブジェクト名をキーとして記憶部３４をルックアップして、該当するキャッシュ・エントリの検索が実行される。該当するキャッシュ・エントリ３６ａが検索された場合には、検索された実行結果がブラウザ・ソフトウエアを使用してユーザへと提供される。検索されなかった場合には、その通知がアクセス制御部３２へと送られ、その後に得られた要求オブジェクトの実行結果の値が、実行されたオブジェクトのオブジェクト名、アクセス権限セットと共にキャッシュ・エントリ３６ｂとして格納される。

Ｄ：オブジェクト・アナライザにおける詳細処理

本発明のオブジェクト・アナライザ２４は、Webサービスを実行するためのオブジェクトが呼び出す可能性のあるメソッドごとにアクセス権限を判断し、オブジェクトーアクセス権限リストを生成する。図１０には、本発明のオブジェクト・アナライザ２４の概略的な処理を示す。図１０（ａ）には、呼び出されるメソッドm_1と、メソッドm_1がさらに呼び出す可能性のあるメソッド$n_1()$～$n_i()$についてのアクセス権限を示している。これらのメソッドに対するアクセス権限は、図８で示したメソッドーアクセス権限テーブルにより与えられる。所定のメソッドm_1に対するアクセス権限は、Webサービス提供者により与えられるメソッドm_1についてのアクセス権限であるpermission(m)、例えばGold、Silver、Bronze、A、X、Y、Zと、メソッドが呼び出す可能性のあるメソッド$n_1()$～$n_i()$に付与されたアクセス権限、例えばメソッド$n_1()$についていえば、{{B,S},{S,G}}とされている。

なお、{{B,S},{S,G}}は、メソッドn_1()にアクセスするためには、アクセス権限が、BまたはSおよびアクセス権限がSまたはGであることを必要とすることを意味する。図１０（ａ）では、メソッドm_1には、{G,A}のアクセス権限が設定され、メソッドm_1が呼び出しを行う可能性ｂのあるメソッドn_1～n_iへのアクセス権限がすべて満たされなければメソッドm_1へのアクセスは認めない。この処理を行った後、結果として生成されるメソッドm_1へのアクセスが認められるためのアクセス権限セットをrequires(m1)で表すと、requires(m1)={{B,S},{G},{X},{Y,Z}}が得られる。上述したrequiresが、アプリケーション－アクセス権限リストにおけるアクセス権限セットを与える。図１０（ｂ）には、本発明の特定の実施の形態におけるアクセス権限セットrequires(m)を得るための論理式を示す。なお、本発明においては、呼び出されるメソッドのうち、アクセス権限が不明である場合には、キャッシュ機構へのアクセスを拒否する構成とすることができる。また、これとは反対に、呼び出されるメソッドのアクセス権限が不明である場合には、キャッシュ機構へのアクセスは認めないが、Webサービスの提供だけはできるように構成することもできる。また、図１０（ｂ）において、unknownとは、アクセス権限が不明のメソッドを意味し、本発明では、アクセス権限が不明のメソッドがあると、キャッシュ・アクセスを拒否する構成とすることができるし、またアクセス権限が不明のメソッドがあっても少なくともWebサービスを実行可能に設定することもできる。このような設定のフレキシビリティは、本願において、オブジェクト・アナライザ２４とキャッシュ機構２２とを、機能的に完全に分離したことにより可能となる。

図１１は、本発明においてオブジェクト・アナライザ２６が実行するアクセス権限をメソッドごとに実行するための処理を示したフローチャ

ートである。オブジェクト・アナライザの処理は、ステップＳ５０から開始し、ます、プログラムが呼び出す可能性のあるメソッドをリストしたメソッド・リスト（todo-list）と、処理を終えたメソッドを格納するための処理済リスト(done-list)とをクリアする。ステップＳ５２では、オブジェクトを解析して得られたメソッドをメソッド・リストに格納する。ステップＳ５４では、メソッド・リストに格納されたメソッドに対して、メソッドーアクセス権限テーブルを参照してアクセス権限を取得する。ステップＳ５６では、メソッド・リストが空になったか否かを判断し、空になった場合（yes）には、呼び出される可能性のあるメソッドに対する処理は終了したので、ステップＳ５８に進んで生成された最終的なアクセス権限セットを生成させる。また、メソッド・リストが空ではない場合(no)には、さらに処理を行うメソッドが残されているので、ステップＳ５４に戻り、処理を反復する。

図１２は、図１１に示したステップＳ５４の処理の詳細なフローチャートを示した図である。処理は、ステップＳ６０から開始し、メソッド・リストからメソッドを抽出する。ステップＳ６２では、抽出されたメソッドにつき、メソッドーアクセス権限テーブルをルックアップしながらメソッドのアクセス権限を取得してメモリに格納する。ステップＳ６４では、抽出したメソッドを処理済リストへと移すと同時に、メソッド・リストから削除する。ステップＳ６６では、メソッド呼出しが行われる可能性のある他のメソッドをメソッド・リストに追加して、ステップＳ５４の判断が、肯定的な結果を返すまで順次処理が実行される。図１３には、図１２において説明した処理を実行させるための特定の実施の形態における擬似コードを示すものの、本発明においては、図１２に示した処理を実行させる擬似コードとしては、同様の機能を達成することが

できるいかなるものでも使用することができる。上述した処理により、本発明においてはコード解析がなされ最終的には、集合変数を含む処理済リストの中にサービスを実行するためにアクセスが必要な（可能性のある）メソッドをすべて列挙することができる。

また、本発明の他の態様においては、メソッドのコード中でinvokevirtualなどのメソッド呼出しをともなう部分を探す方法を採用することにより、フロー解析を直接実行させずにメソッドをメソッド・リストに含ませることができる。本発明の上述した他の態様の処理を図１４に示す。具体的には、メソッド呼び出しに指定されたオブジェクトの静的なクラスやインターフェースに加え、そのサブクラスについて、呼び出されているメソッドが呼ばれるとみなすことにより、処理を実行させることができる。例えば、天気予報の情報提供サービスで説明したWeather型のオブジェクトに対しgetInfo()が呼び出され、Weatherのサブクラスに WeatherImplがあるものとする。このとき、WeatherクラスのgetInfo()に加えて、WeatherImplクラスのgetInfo()も呼び出される可能性のあるメソッドであるとみなして、メソッド・リストに含ませることができる。また、本発明は、コントロール・フロー解析やデータ・フロー解析を行なうことで、これらのフロー解析を実行させないで得られるメソッド群から、呼出される可能性のないメソッド群を取り除く処理を追加することもできる。

Ｅ：アクセス制御部におけるアクセス権限判断の詳細処理

図１５には、本発明のアクセス制御部における詳細な処理のフローチャートを示す。アクセス権限判断の処理は、まずステップＳ７０において、アクセス許可フラグを初期化（偽）に設定する。ステップＳ７２に

おいて、要求するオブジェクトにつき、オブジェクトーアクセス権限リストにおけるアクセス権限セットのうちの最初のセットをメモリから読み出す。ステップＳ７４において、ユーザのアクセス権限と、読出されたセットとの比較を実行し、比較結果をメモリに格納させる。ステップＳ７６において、比較結果をメモリから読出し、値が偽であるか否かを判断する。比較結果が偽である場合（yes）には、少なくとも１つのセットのアクセス権限をユーザは保有しないので、ステップＳ７８において処理を終了させる。この場合、アクセス許可フラグは、nullのまま保持される。また、比較結果が偽でない場合(no)には、ステップＳ８０においてすべてのセットを判断したか否かを判断し、すべてのセットを判断していない場合(no)には、ステップＳ７４に戻って次のセットをメモリから読み出し、ステップＳ７６の判断を実行させる。

ステップＳ８０においてアクセス権限セットすべてを判断した場合（yes）には、アクセス権限セットを構成するすべてのセットに対してユーザがアクセス権限を保有しているので、ステップＳ８２へと進んで、アクセス許可フラグを設定し、ユーザＩＤおよびオブジェクトを指定して記憶部３４へのアクセスを可能とさせる。図１６は、図１５に示したフローチャートのうち、ステップＳ７４～ステップＳ８０における判断処理を、ユーザが保有するアクセス権限をｐとし、アクセス権限セットが、（Ａ，Ｂ）、（Ｂ，Ｃ）、（Ｘ，Ｙ，Ｚ）である場合について実行させる際の擬似コードを示すが、本発明においては図１３において説明したように、同様の機能を実現するいかなるコーディングでも使用することができる。

図１７は、本発明のWebサービス提供システムにおけるユーザ端末１２

と、サーバ装置装置１４との間の要求と応答のシーケンスを示した図である。図１７では、ユーザ端末１２からオブジェクト呼出し要求を発行されており、要求管理部３０は、オブジェクト呼出し要求を受け取って、アクセス制御部３２に対してアクセス権限の判断を要求している。アクセス制御部３２は、ユーザーアクセス権限リストをルックアップして、ユーザのアクセス権限を判断し、アクセス権限があると判断すると、記憶部３４に対してキャッシュ・エントリの検索を実行させる検索要求を発行している。図１７において示した実施の形態では、該当するキャッシュ・エントリが見出されず、nullの応答がアクセス制御部３２に返されている。

アクセス制御部３２は、キャッシュ・エントリがない通知を受け取り、要求管理部３０に対して、オブジェクト呼出し許可の通知を渡す。この通知を受け取った要求管理部３０は、オブジェクト呼出し要求を、オブジェクト実行部２６に渡し、処理を実行させる。実行結果は、要求管理部３０が取得し、要求管理部３０は、実行結果をユーザに提供する。また、アクセス制御部３２は、記憶部３４への格納要求を発行して、新たな実行結果を格納させている。

図１８は、本発明のWebサービス提供システムにおける要求ー応答シーケンスの他の実施の形態を示した図である。図１８では、ユーザ端末１２からオブジェクト呼出し要求を発行しており、要求管理部３０は、オブジェクト呼出し要求を受け取って、アクセス制御部３２に対してアクセス権限の判断を要求している。アクセス制御部３２は、ユーザーアクセス権限リストをルックアップしてアクセス権限を判断し、アクセス権限があると判断して記憶部３４に対してキャッシュ・エントリの検索を

実行させる要求を発行している。

図１８において示した実施の形態では、キャッシュ・エントリが見出され、キャッシュ・エントリの値を要求管理部３０へと取得させ、キャッシュ・エントリの値がサービス応答の結果としてユーザに提供されている。図１８に示されるように本発明においては、キャッシュ・エントリの値をユーザに返すまでの間にアクセス権限の判断を実行するので、キャッシュ・エントリへのセキュリティを向上させると共に、ユーザに対するWebサービスの提供を高速化することが可能となる。

図１９は、本発明のWebサービス提供システムにおけるユーザ端末１２と、サーバ装置装置１４との間の要求と応答のシーケンスのさらに他の実施の形態を示した図である。図１９に示した実施の形態は、例えば、ユーザが以前にWebサービスに対して互いアクセス権限のサービスを受けたものの、その後アクセス権限が変化した場合や、Webサービスの提供者側の理由により、所定のアクセス権限でのWebサービスの種類を変更した場合に生じる。

図１９では、ユーザ端末１２からオブジェクト呼出し要求を発行している。要求管理部３０は、オブジェクト呼出し要求を受け取って、アクセス制御部３２に対してアクセス権限の判断を要求している。アクセス制御部３２は、ユーザーアクセス権限リストをルックアップしてアクセス権限を判断している。図１９において示した実施の形態では、該当するキャッシュ・エントリが見出され、キャッシュ・エントリの値がアクセス制御部３２に返されている。図１９に示した実施の形態では、アクセス制御部３２がその時点でのユーザがキャッシュ・エントリにアクセ

スする権限がないと判断し、キャッシュ・エントリに対するアクセス権限がないアクセス拒否の通知を発行し、要求管理部３０は、この通知を受け取っている。

この通知を受け取った要求管理部３０は、ユーザに対してアクセス拒否を通知している。この通知を受け取ったユーザは、再度別のオブジェクト呼出し要求を送り、サーバ装置１４は、図１７～図１９に示した処理を選択的に反復させ、ユーザとのトランザクションを進行させることになる。図１９に示される実施の形態のように、本発明においては、ユーザ側のアクセス権限の変動およびWebサービスの条件変更に対して最小のソフトウエアおよびハードウエア資源で迅速に対応でき、高速、かつ高信頼性のWebサービスの提供を行うことが可能となる。

本発明の形態では、上述したようにアクセス権限セットとして、単純にアクセス権限を要素に持つ集合を要素とする集合として構成することも可能であるし、アクセス権限を要素に持つ集合ＲとＳとがあり得る場合に、Ｒのアクセス権限のどれかを持っているならばＲのアクセス権限のどれかを保持することが知られている場合、アクセス権限セットＲのみを保持するようにすることもできる。例えば、Ｒが{Gold}で、Ｓが{Gold,Silver}の場合には、Ｒのアクセス権限がある場合にはＳを含ませないようにしてアクセス権限セットを構成させることもできる。

さらに本発明の他の実施の形態では、サーバ装置装置の管理者が、サービスがWebサービスのオブジェクトのコード解析結果に関わらず、そのサービスの結果をキャッシュさせるように指定することができる。

例えば、あるメソッドgetWeatherForecast()は、コード解析を用いるとアクセス制御機構によりキャッシュ結果を返してはいけないという判定が下されるとする。この場合には通常では、getWeatherForecast()のリクエストに対しては常に実際にWebサービス・オブジェクトが呼び出される。このような場合でも、管理者が特定の限定されたユーザに対して「getWeatherForecast()の結果はキャッシュしてよい」という指定をアプリケーション・サーバ装置に与えることによって、後続するgetWeatherForecast()のリクエストに対してキャッシュされた結果が返されるようにすることを可能とする。キャッシュ機構はこのような設定が与えられている場合には、本発明では、オブジェクト・アナライザと、アクセス制御部とが独立して構成されているので、要求に対応するキャッシュ・エントリがあったときはアクセス制御部の判断によらず、キャッシュ・エントリの値を実行結果としてユーザに返す構成とすることもできる。

図２０には、本発明のさらに別の実施の形態を示す。図２０に示した本発明の他の実施の形態では、エッジ・サーバ装置５０に記憶部３４として使用することもできる。すなわち、本発明の可能な実施の形態では、本発明のキャッシュ機構は、アプリケーション・サーバ装置５２とは別のエッジ・サーバ装置５０に配置される。このようなエッジ・サーバ装置５０は、ユーザとアプリケーション・サーバ装置５２との間に配置されることで、ユーザに対し複数のアプリケーション・サーバ装置への統一したインターフェースを提供することができる。エッジ・サーバ装置５０は、ユーザからの要求を受け付け、その要求に含まれる処理をアプリケーション・サーバ装置５２に依頼し、エッジ・サーバ装置５０に戻された結果をユーザへと返す構成とすることができる。

エッジ・サーバ装置のキャッシュ機構２２は、上述したアプリケーション・サーバ装置５２の結果をキャッシュしておき、ユーザ要求に応じてキャッシュされた結果を返す構成とすることもできる。上述したエッジ・サーバ装置におけるアクセス制御つきキャッシュ機構においても、サーバ装置装置１２内に含ませたキャッシュ機構と処理の実施の形態は、大きく変わるものではなく、キャッシュ機能２２と、プログラム実行部２４との間の通信が、例えばＴＣＰ／ＩＰプロトコルを介したインターネットや、ＬＡＮ、ＷＡＮといったネットワークを介して行われている。

本発明の上述した各機能を実現する手段または部分は、コンピュータ実行可能なプログラム言語により記述されたソフトウエアまたはソフトウエア・モジュール群として構成することができ、必ずしも図面に記載した機能ブロックとして構成される必要はない。また、本発明のWebサービス提供システムでは、要求されるテーブルは必要に応じていかなる機能モジュールと共に構成することができ、本発明の図面に示された特定の実施の形態に限定されるものではない。

本発明のプログラムは、種々のプログラミング言語、例えばJava（登録商標）Beansなどを使用して記述することができ、本発明のプログラムを記述したコードは、磁気テープ、フレキシブル・ディスク、ハードディスク、コンパクト・ディスク（ＣＤ）、光磁気ディスク、デジタル・バーサタイル・ディスク（ＤＶＤ）といったコンピュータ可読な記録媒体に保持させることができる。

上述したように、本発明は、高い信頼性で、高付加価値のWebサービス

を可能な限り迅速に提供することを可能とするWebサービス提供システムを提供することを可能とする。さらに本発明は、コンピュータ・システムを上述したWebサービスを提供することができるサーバ装置装置を提供することを可能とする。さらに本発明は、コンピュータ・システムを上述したサーバ装置装置として機能させることが可能なサーバ装置制御方法を提供することを可能とする。また本発明のさらに別の目的は、コンピュータ・システムを上述したサーバ装置装置として機能させるためのプログラム、および該プログラムを記録したコンピュータ可読な記録媒体を提供することを可能とする。

請求の範囲

1. ネットワークを介してWebサービスを提供するためのサーバ装置を含むWebサービス提供システムであって、前記サーバ装置は、前記ネットワークを介して受信したオブジェクト呼出し要求と、ユーザ識別子とを取得すると共に、取得したオブジェクト呼出し要求を格納させ、かつ前記ユーザ識別子により指定されるアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、過去に実行されたオブジェクトの実行結果を格納する記憶部とを含み、前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、Webサービス提供システム。

2. 前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させる、請求項1に記載のWebサービス提供システム。

3. 前記サーバ装置はさらに、オブジェクト実行手段を含み、前記制御手段は、前記記憶部に該当する過去の実行結果が格納されていない場合に、前記オブジェクト呼出し要求をオブジェクト実行部に送り前記要求オブジェクトを実行させる、請求項1に記載のWebサービス提供システム。

4. 前記サーバ装置は、前記制御手段を含むエッジ・サーバと、前記

オブジェクト実行部を含むアプリケーション・サーバとから構成される、請求項３に記載のWebサービス提供システム。

５．　ネットワークを介してWebサービスを提供するためのサーバ装置であって、前記サーバ装置は、オブジェクト呼出し要求を受取り、かつ格納させると共に、要求オブジェクトへのアクセス権限と、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限セットとを比較する制御手段と、過去に実行されたオブジェクトの実行結果を格納する記憶部とを含み、前記制御手段は、前記記憶部が過去に実行された前記要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信する、サーバ装置。

６．　前記制御手段は、前記ユーザ識別子により指定されるアクセス権限が前記アクセス権限セットに含まれる場合に、前記記憶部の検索を実行させる、

請求項５に記載のサーバ装置。

７．　ネットワークを介してWebサービスを提供するためのサーバ装置であって、前記サーバ装置は、要求オブジェクトが呼出す可能性のあるメソッドすべてを取得してアクセス権限セットを生成するオブジェクト・アナライザ手段と、前記要求オブジェクトを実行するためのオブジェクト実行手段と、過去のオブジェクトの実行結果を格納する記憶部を含んで構成され、かつ前記アクセス権限セットを使用して前記オブジェクト呼出し要求に応答して前記記憶部に対するアクセス制御を実行するキャ

ッシュ機構とを含むサーバ装置。

８． 前記キャッシュ機構は、要求管理部と、前記記憶部に格納された過去の要求オブジェクトの実行結果の検索を制御するアクセス制御部とを含んで構成される請求項７に記載のサーバ装置。

９． 前記アクセス制御部は、前記要求オブジェクトに対するアクセス権限と、前記アクセス権限セットとを比較してアクセス制御を実行し、前記要求管理部は、前記アクセス制御部の判断に応答して前記オブジェクト呼出し要求を前記オブジェクト実行部へと渡して前記要求オブジェクトの実行を制御する、請求項８に記載のサーバ装置。

１０． 前記オブジェクト・アナライザ手段は、さらにオブジェクトのコードから前記オブジェクトが呼出す可能性のあるメソッドを取得する手段と、該メソッドに対応するアクセス権限を取得する手段と、前記オブジェクトが呼び出す可能性のあるすべてのメソッドへのアクセス権限から前記アクセス権限セットを生成して格納させる手段とを含む請求項７に記載のサーバ装置。

１１． 前記キャッシュ機構を含むエッジ・サーバと、前記オブジェクト実行手段と、前記オブジェクト・アナライザ手段とから構成されるアプリケーション・サーバとを含んで構成される、請求項７に記載のサーバ装置。

１２． コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのサーバ制御方法で

あって、前記方法は、前記コンピュータ・システムに対して、オブジェクト呼出し要求を受信し格納するステップと、要求オブジェクトへのアクセス権限をメモリから取得するステップと、前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記要求オブジェクトの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップとを実行させる、サーバ制御方法。

１３．　前記記憶部が過去に実行された要求オブジェクトの実行結果を格納する場合には、前記要求オブジェクトの実行前に前記格納された過去の要求オブジェクトの実行結果を前記ネットワークを介して前記サーバ装置の外部に送信するステップを実行させる、請求項１２に記載の方法。

１４．　前記記憶部が過去に実行された要求オブジェクトの実行結果を格納しない場合には、前記オブジェクト呼出し要求をオブジェクト実行部へと渡すステップを実行させる、請求項１２に記載の方法。

１５．　コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、オブジェクト呼出し要求を受信し格納するステップと、要求オブジェクトへのアクセス権限をメモリから取得するステップと、前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、

前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップとを実行させる、プログラム。

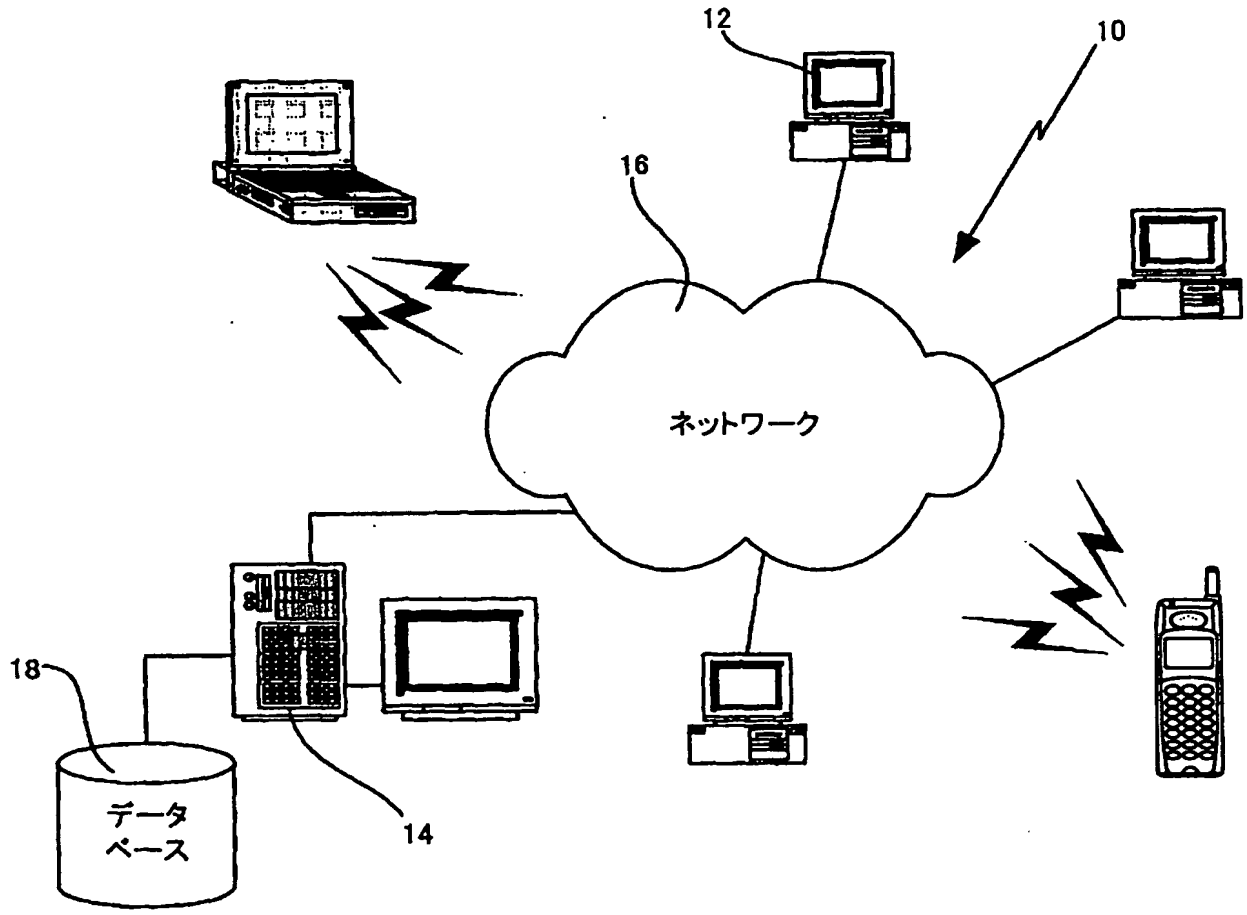
１６．　前記記憶部が過去に実行された要求オブジェクトの実行結果を格納する場合には、前記検索された実行結果を前記サーバ装置の外部へと送信するステップを実行させる、請求項１５に記載のプログラム。

１７．　前記記憶部が過去に実行された要求オブジェクトの実行結果を格納しない場合には、前記オブジェクト呼出し要求をオブジェクト実行部へと渡すステップを実行する、請求項１５に記載のプログラム。

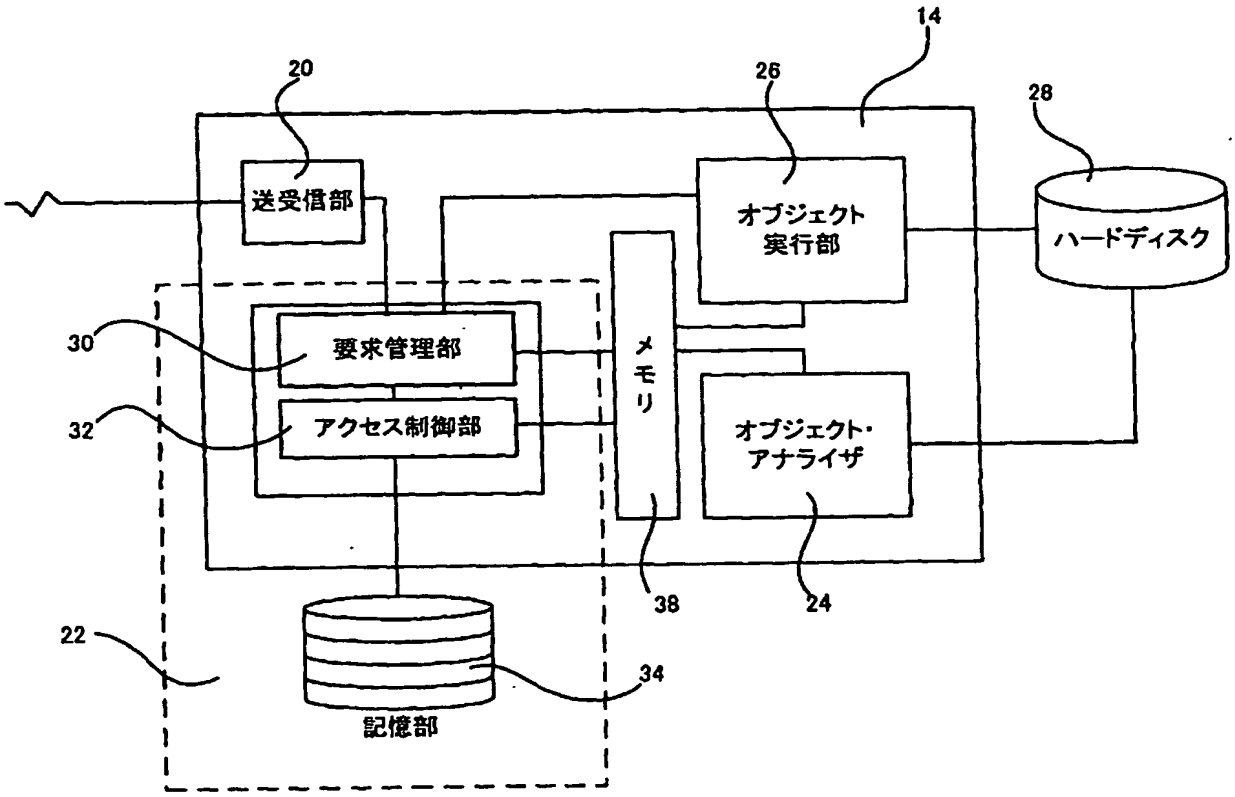
１８．　コンピュータ・システムを、ネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対して、オブジェクト呼出し要求を受信し格納するステップと、要求オブジェクトへのアクセス権限をメモリから取得するステップと、前記要求オブジェクトの実行を行うためのアクセス権限セットをメモリから読出すステップと、前記アクセス権限が前記アクセス権限セットに含まれるか否かを判断するステップと、前記アクセス権限が前記アクセス権限セットに含まれる場合には、前記アプリケーションの実行前に過去のオブジェクトの実行結果を格納した記憶部を検索させるステップとを実行させる、コンピュータ可読な記憶媒体。

１９．　コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムは、前記コンピュータ・システムに対して、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップとを実行させるプログラム。

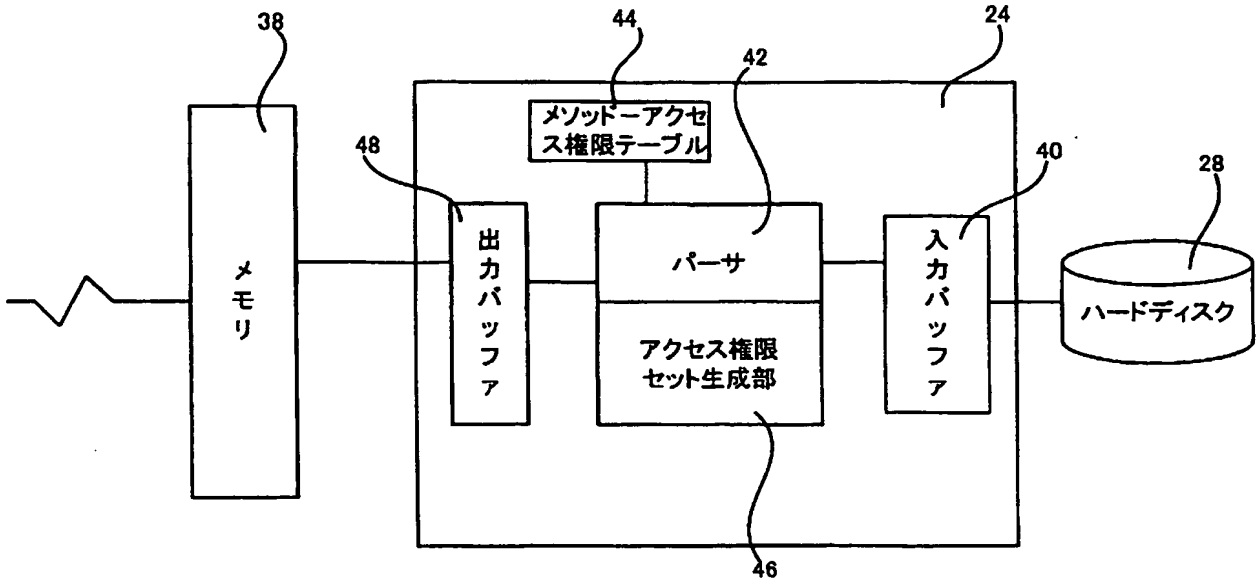
２０．　コンピュータ・システムをネットワークを介してWebサービスを提供するためのサーバ装置として機能させるためのプログラムであって、前記プログラムを記憶したコンピュータ可読な記憶媒体であって、前記プログラムは、前記コンピュータ・システムに対して、要求オブジェクトが呼出す可能性のあるメソッドすべてに対するアクセス権限から生成されるアクセス権限セットをメモリから読出すステップと、前記要求オブジェクトに対する所与のアクセス権限と前記アクセス権限セットとを使用して記憶部に格納されたオブジェクトの過去の実行結果へのアクセスを制御するステップとを実行させる記憶媒体。



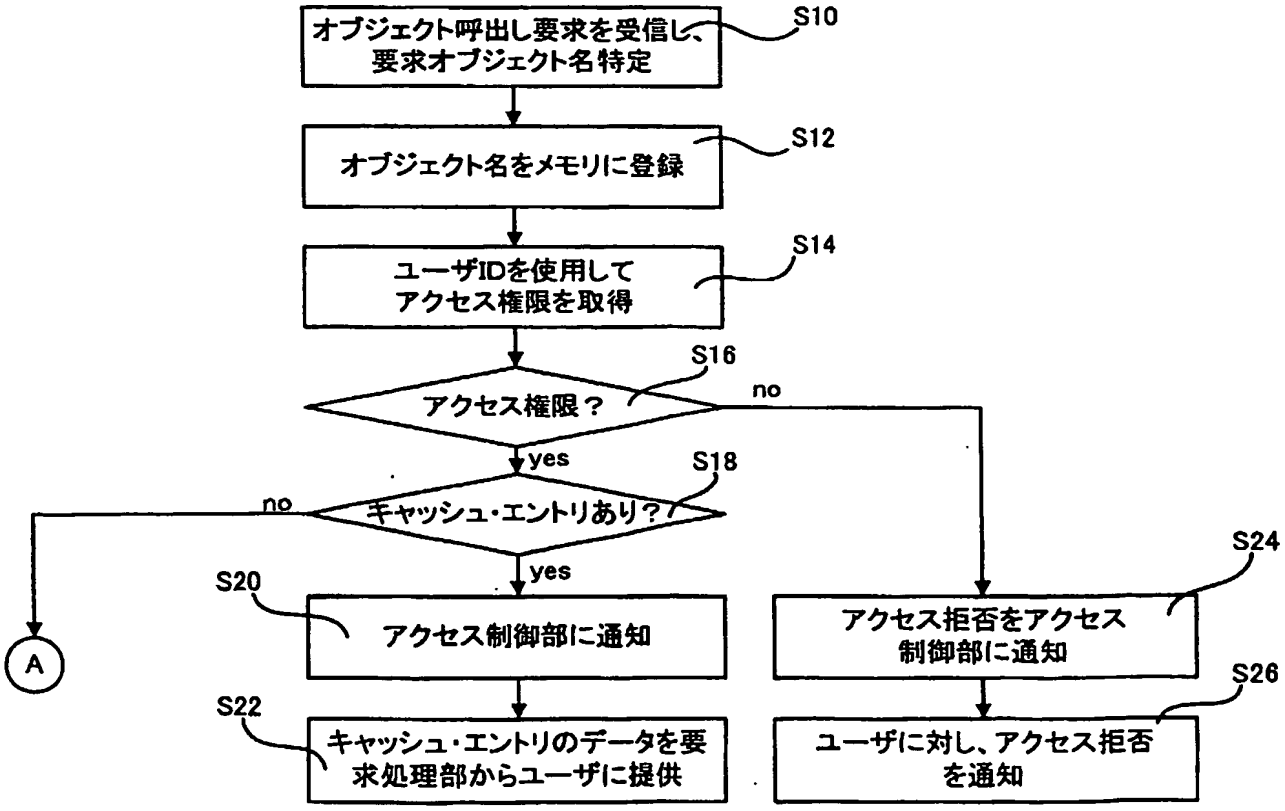
第 1 図


14
20
26
28
送受信部
オブジェクト
実行部
ハードディスク
30
要求管理部
メモリ
32
アクセス制御部
オブジェクト・
アナライザ
38
24
22
34
記憶部

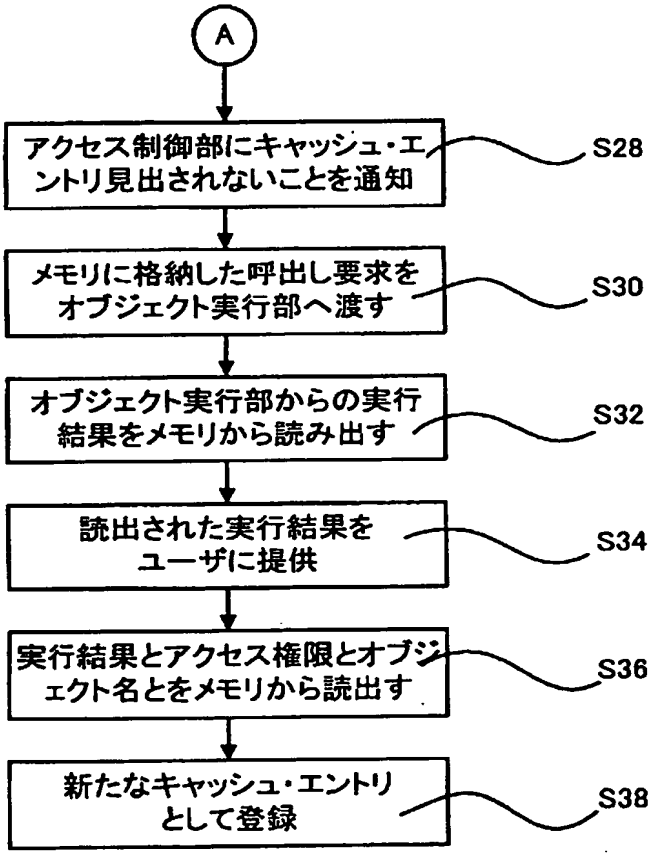
第 2 図


38
44
42
24
メソッドーアクセス権限テーブル
48
40
28
メモリ
出力バッファ
パーサ
アクセス権限セット生成部
入力バッファ
ハードディスク
46

第 3 図


オブジェクト呼出し要求を受信し、要求オブジェクト名特定
S10
オブジェクト名をメモリに登録
S12
ユーザIDを使用してアクセス権限を取得
S14
アクセス権限？
S16
no
yes
キャッシュ・エントリあり？
S18
no
yes
A
S20
アクセス制御部に通知
S22
キャッシュ・エントリのデータを要求処理部からユーザに提供
S24
アクセス拒否をアクセス制御部に通知
S26
ユーザに対し、アクセス拒否を通知

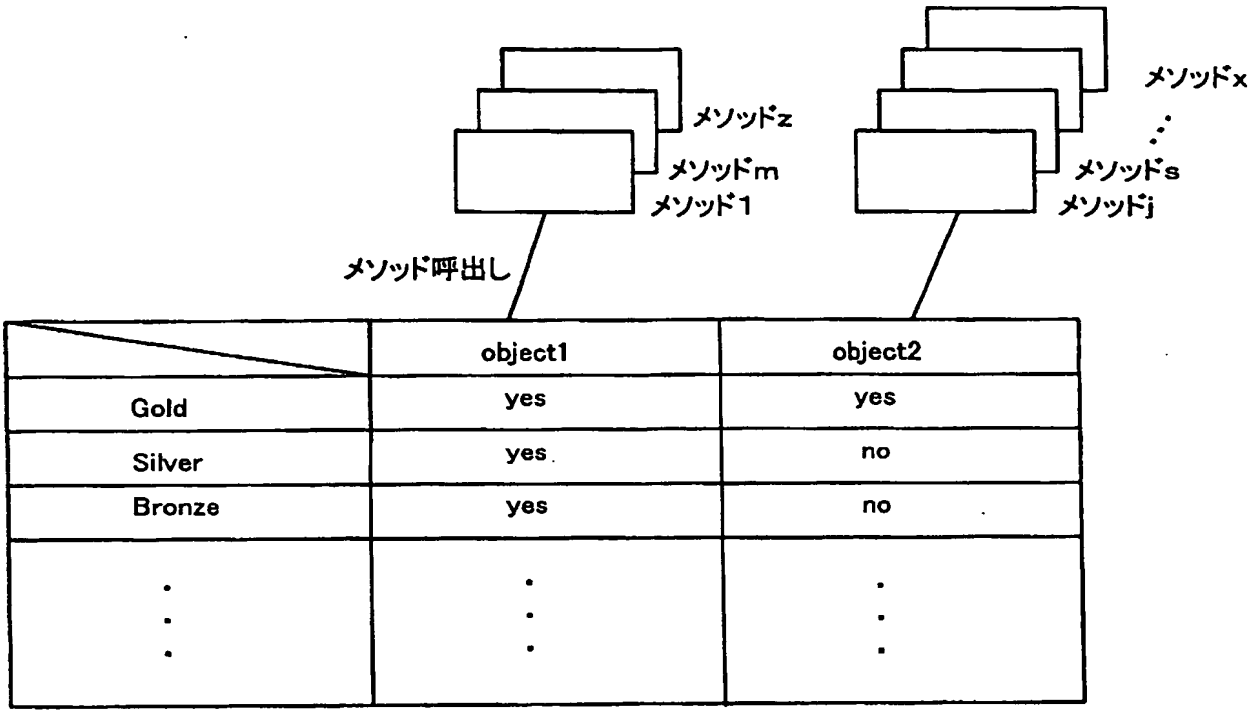
第 4 図


A
アクセス制御部にキャッシュ・エントリ見出されないことを通知
S28
メモリに格納した呼出し要求をオブジェクト実行部へ渡す
S30
オブジェクト実行部からの実行結果をメモリから読み出す
S32
読出された実行結果をユーザに提供
S34
実行結果とアクセス権限とオブジェクト名とをメモリから読出す
S36
新たなキャッシュ・エントリとして登録
S38

第 5 図

ユーザID	アクセス権限	
usdxxhnm	gold	A, C, D, ···, X
usboojkn	gold	A, B, M, ···, X
bbiooean	bronz	B, C, M, ···, Y,Z
⋮	⋮	⋮
xjmbiwmka	silver	B, J, M, ···, X,Z
Ibm123trl	bronz	D, E, F, ···, O,...

第 6 図



	object1	object2
Gold	yes	yes
Silver	yes	no
Bronze	yes	no
. . .	. . .	. . .

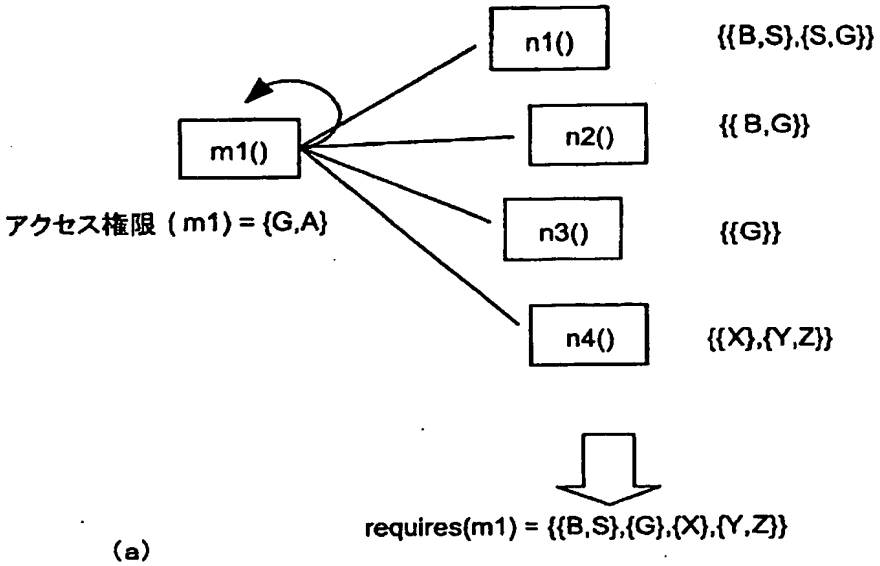
第 7 図

	Method 1	Method 2	...	Method i
Gold	yes	yes		yes
Silver	yes	no		yes
Bronze	no	no		no
A	yes	yes		yes
B	no	yes		no
C	no	no		no
. . .	. . .	. . .		

第 8 図

オブジェクト名	アクセス権限セット	実行結果	
getweatherForecast ()	{(G,S),…,(A)}	実行結果1	36b
getweatherForecast ()	{(B), (A)}	実行結果2	
getDetailedInfo ()	{(G),…,(X,Y,Z)}	実行結果3	36a
getStockRecommendation ()	{(G,B), (S), …, (Y)}	実行結果4	
getStockRecommendation ()	{(S), (S,B), …, (Y)}	実行結果5	36
⋮	⋮	⋮	

第 9 図



(a)

$$requires\ (m) \cong \{\ permission\ (m)\} \oplus \bigcup_i^{\oplus} requires\ (n_i)$$

$$A \oplus B \cong \{r \in A \cup B \mid \neg(\exists s \in A \cup B; r \prec s)\}$$

$$r \prec s \Leftrightarrow r \cup s = s \wedge r \neq s$$

$$\bigcup_i^{\oplus} N_i \cong N_1 \oplus N_2 \oplus \ldots \oplus N_n$$

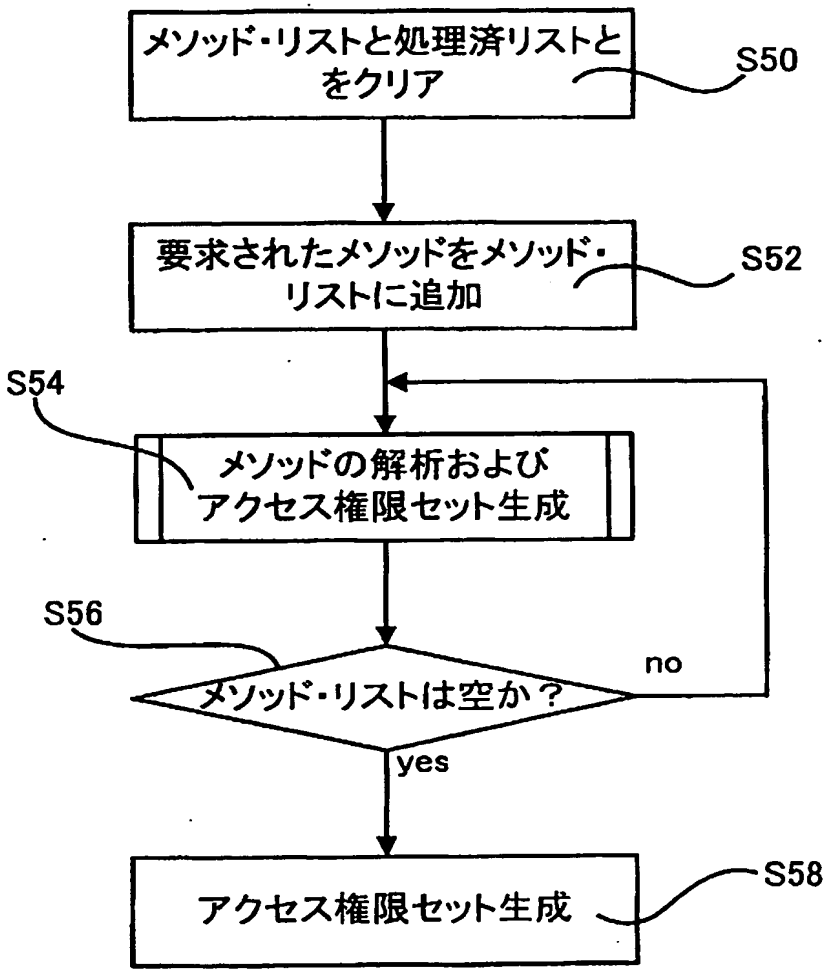
$$unknown\ (m) \Rightarrow permission\ (m) \cong \varnothing$$

$$safe\ (m) \Leftarrow \forall r \in requires\ (m); r \cap p \neq \varnothing$$

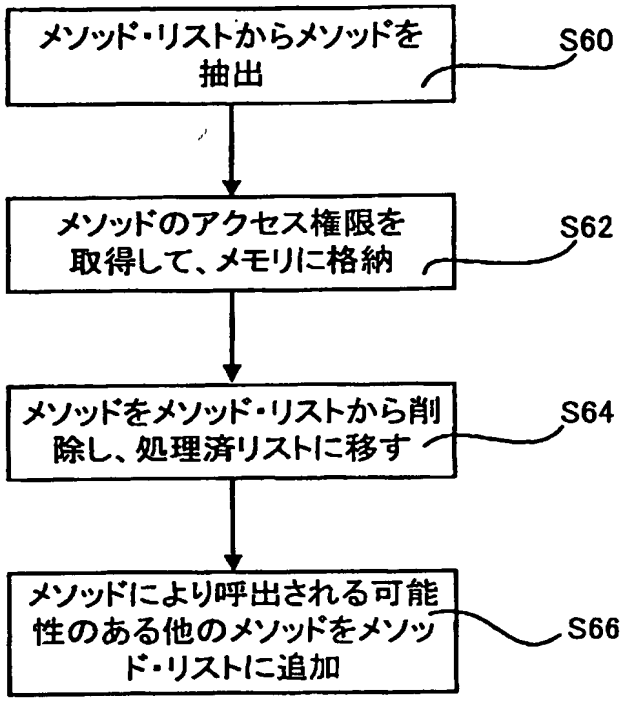
p := the roles - set of an accessing principal

(b)

第 1 0 図


メソッド・リストと処理済リストとをクリア
S50
要求されたメソッドをメソッド・リストに追加
S52
S54
メソッドの解析およびアクセス権限セット生成
S56
メソッド・リストは空か？
no
yes
アクセス権限セット生成
S58

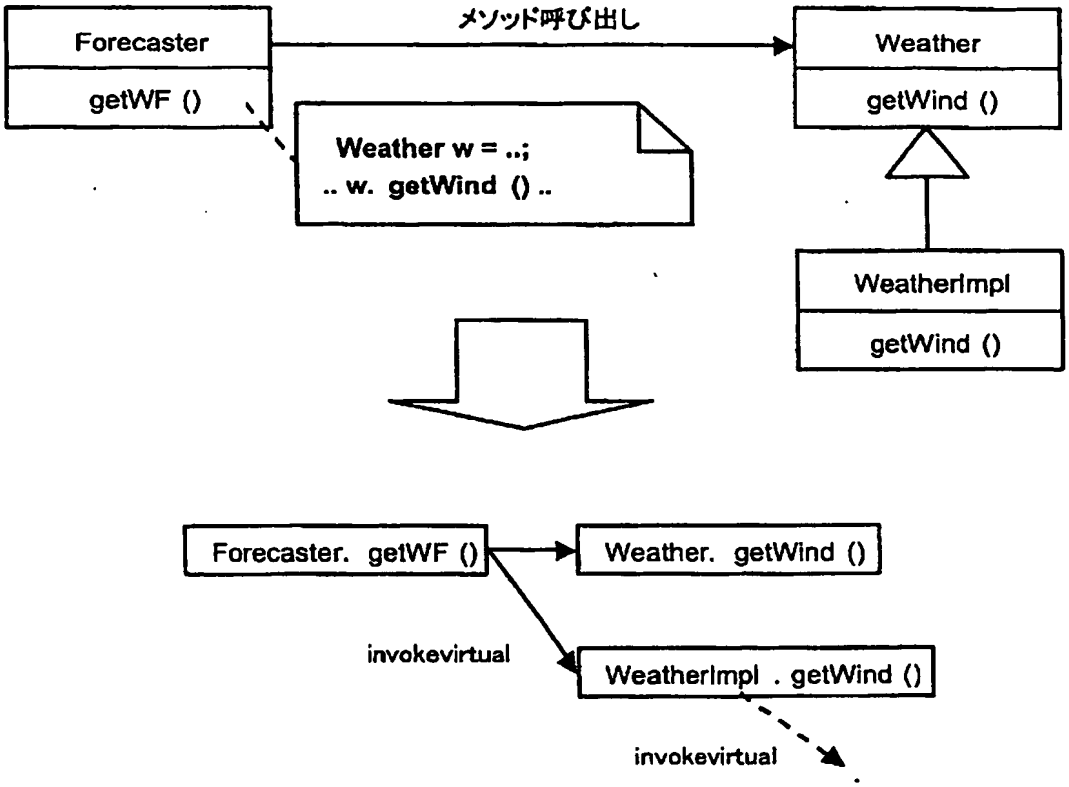
第１１図



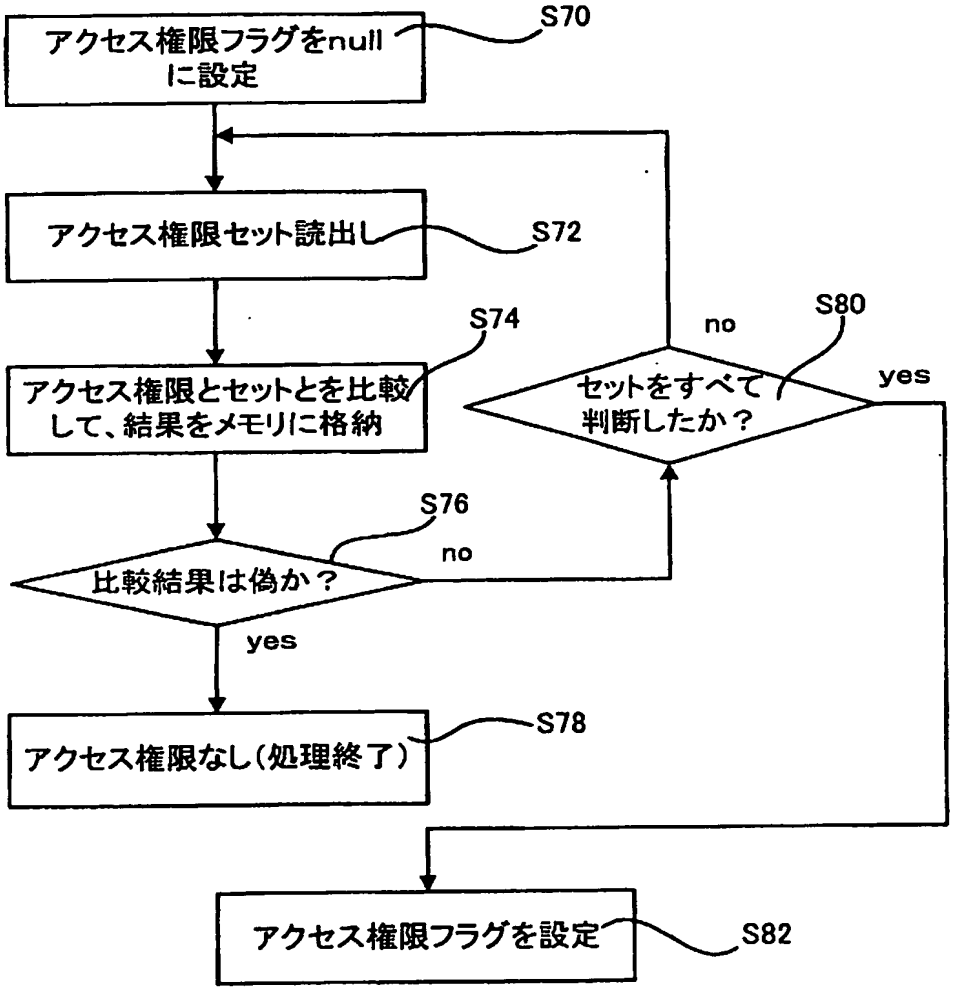
第１２図

```
Set<Method> todo-list = {}
Set<Method> done-list = {}
Set<Set<Role>> result = {}

requiredRoles (method)

requiredRoles(Method m) {
  Set<Set<Role>> result = {}
  foreach Method n in depends(m) {
     if (n not in done-list) {
          add n to done-list
          add roles allowed for n to result (maybe by taking an optimized form)
          // may optimize result
          requiredRoles(n)
     }
  }
}

Set<Set<Role>> represents a set of a set of Role sets.

The depends() returns all of methods that may be directly invoked from the given method.
```

第１３図


Forecaster
getWF ()
メソッド呼び出し
Weather
getWind ()
Weather w = ..;
.. w. getWind () ..
WeatherImpl
getWind ()
Forecaster. getWF ()
Weather. getWind ()
invokevirtual
WeatherImpl . getWind ()
invokevirtual

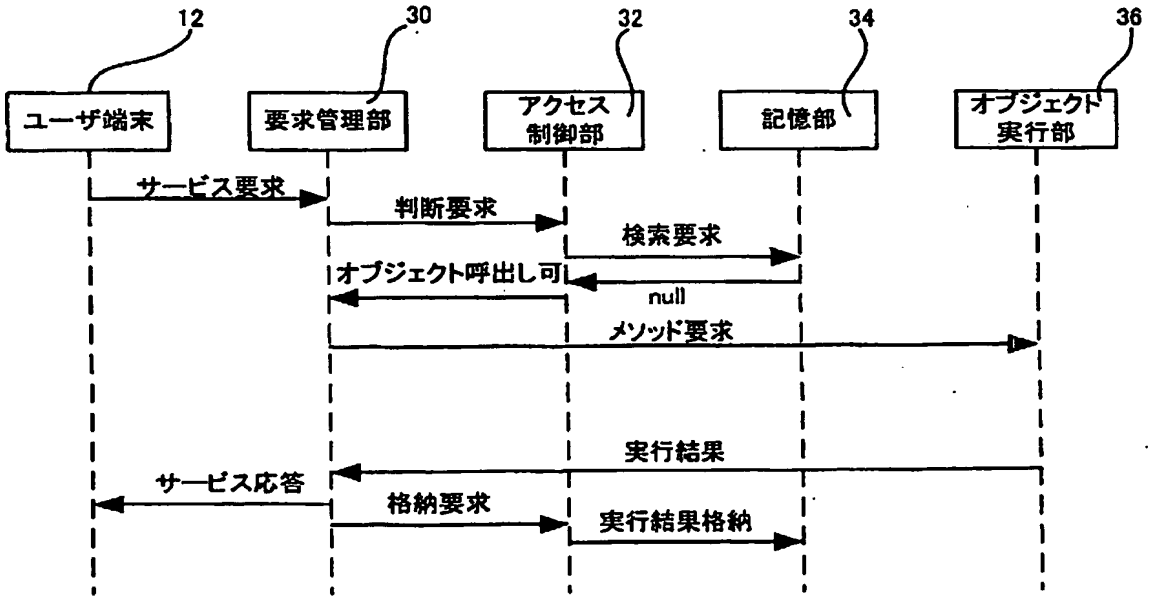
第 1 4 図


アクセス権限フラグをnull
に設定
S70
アクセス権限セット読出し
S72
アクセス権限とセットとを比較
して、結果をメモリに格納
S74
比較結果は偽か？
S76
no
yes
セットをすべて
判断したか？
S80
no
yes
アクセス権限なし(処理終了)
S78
アクセス権限フラグを設定
S82

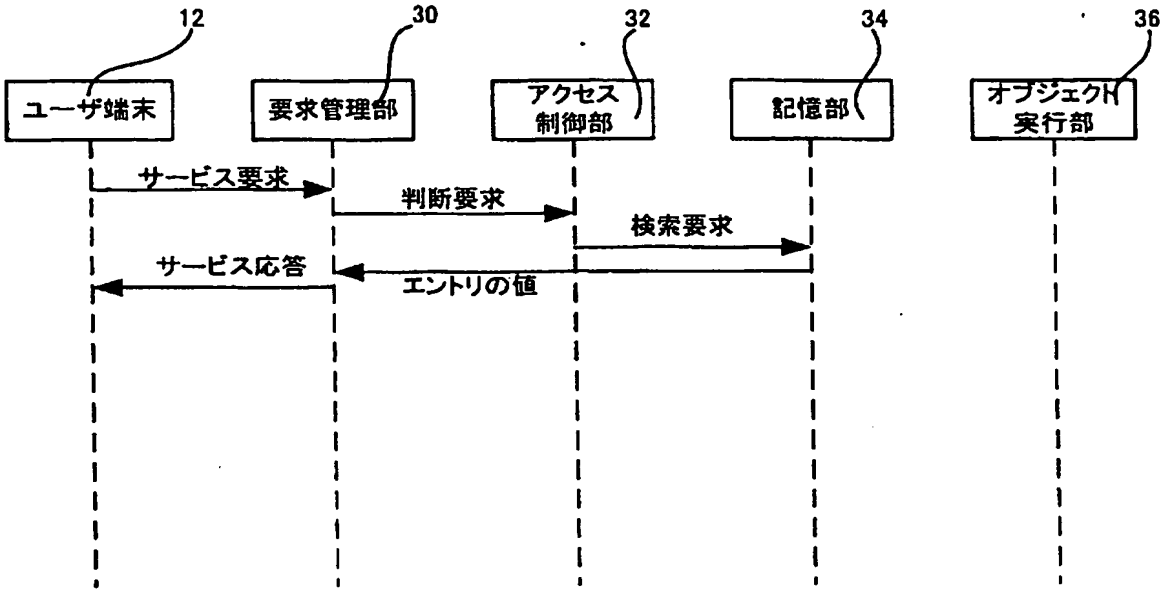
第１５図

```
Principal p
Set<Set<Role>> roleCondition = { (A, B), (B, C), (X, Y, Z) }

if compliesWith(roleCondition) then success else failure

boolean compliesWith(Set<Set<Role>> roleCondition) {
      foreach Set<Role> allowedRoles in roleCondition {
         if not isInAnyOf(allowedRoles) return false
      }
      return true
}

boolean isInAnyOf(Set<Role> allowedRoles) {
      foreach Role role in allowedRoles {
        if p in role then return true
      }
      return false
}
```

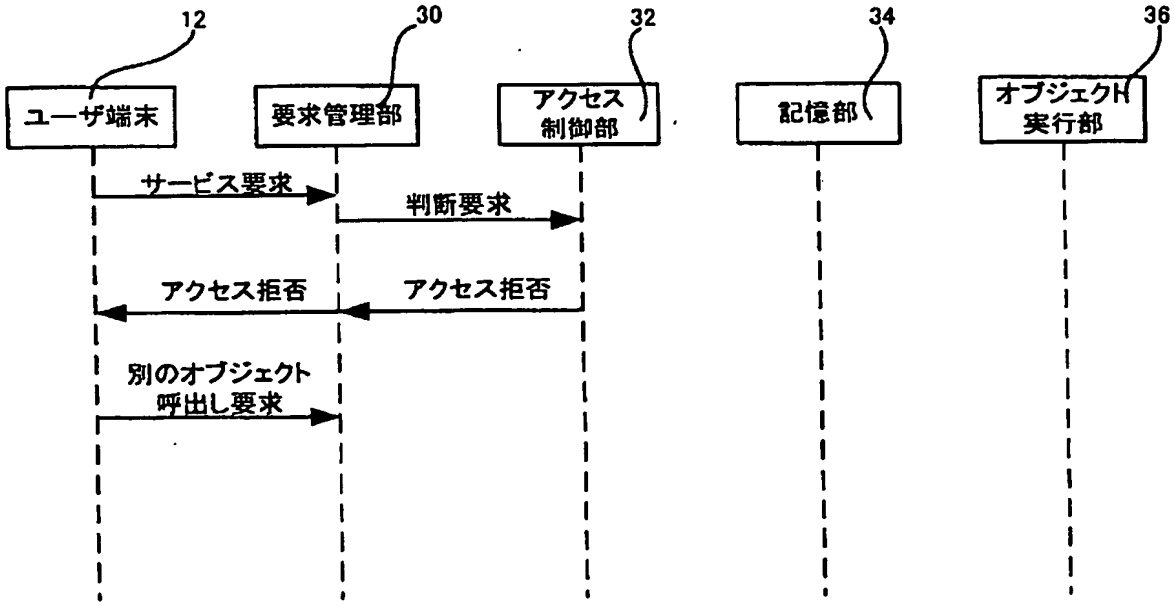
第 １ ６ 図



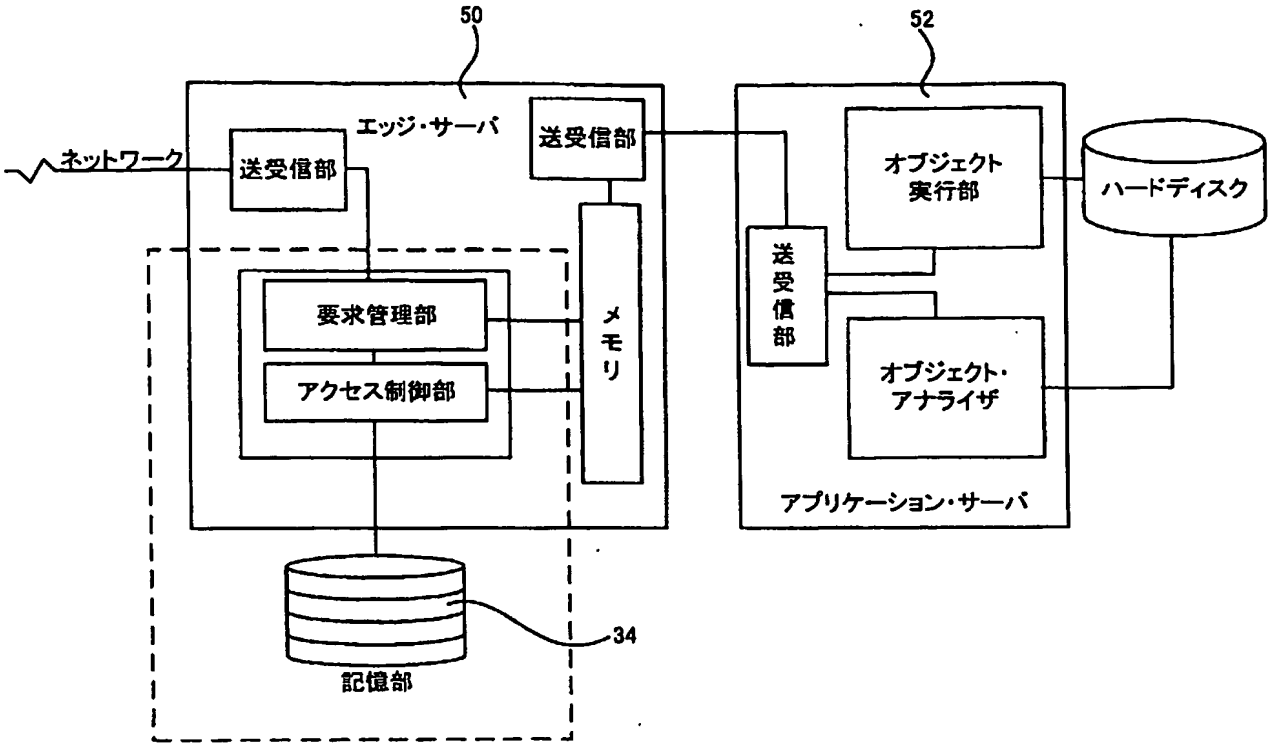
第 １ ７ 図


12
30
32
34
36
ユーザ端末
要求管理部
アクセス制御部
記憶部
オブジェクト実行部
サービス要求
判断要求
検索要求
サービス応答
エントリの値

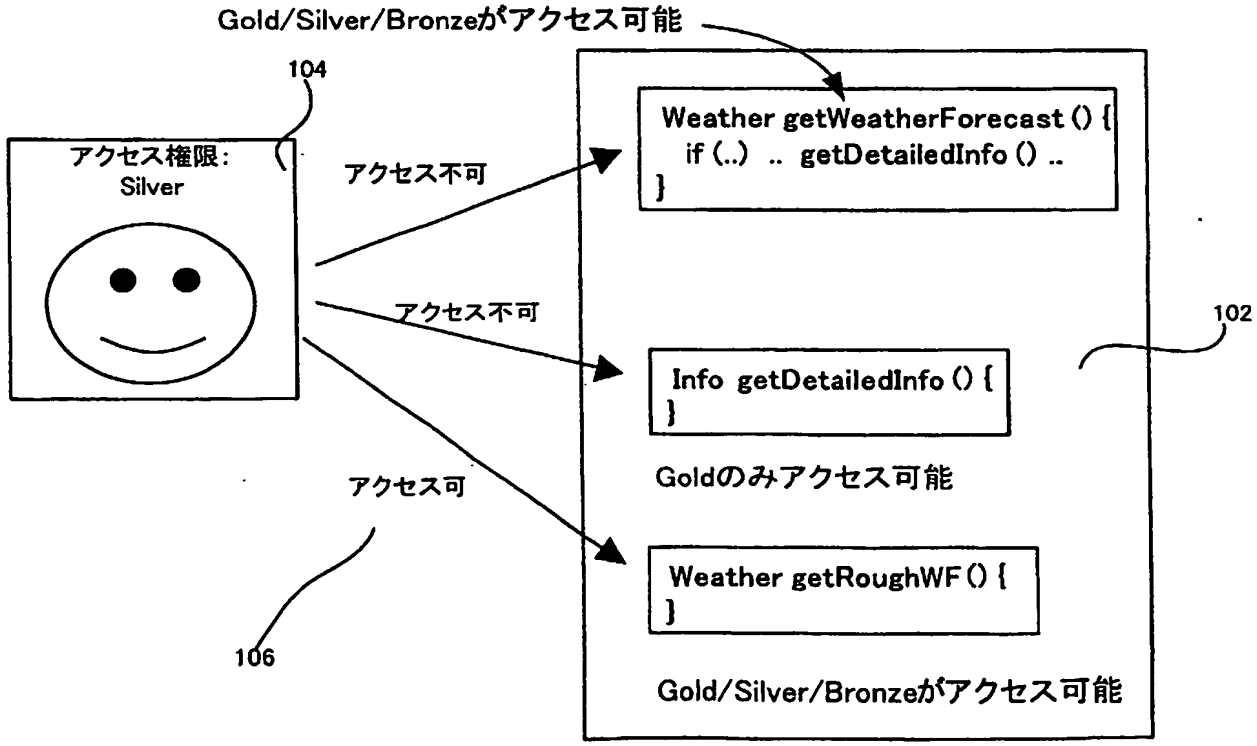
第１８図


12
30
32
34
36
ユーザ端末
要求管理部
アクセス制御部
記憶部
オブジェクト実行部
サービス要求
判断要求
アクセス拒否
アクセス拒否
別のオブジェクト呼出し要求

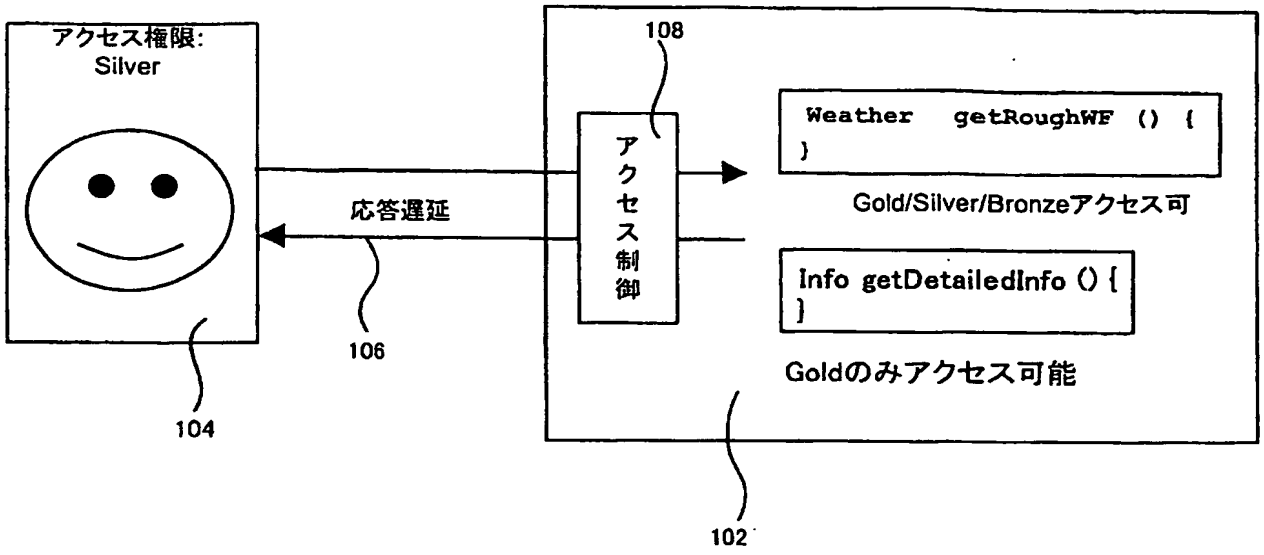
第１９図


50
52
エッジ・サーバ
ネットワーク
送受信部
送受信部
要求管理部
アクセス制御部
メモリ
記憶部
34
送受信部
オブジェクト実行部
ハードディスク
オブジェクト・アナライザ
アプリケーション・サーバ

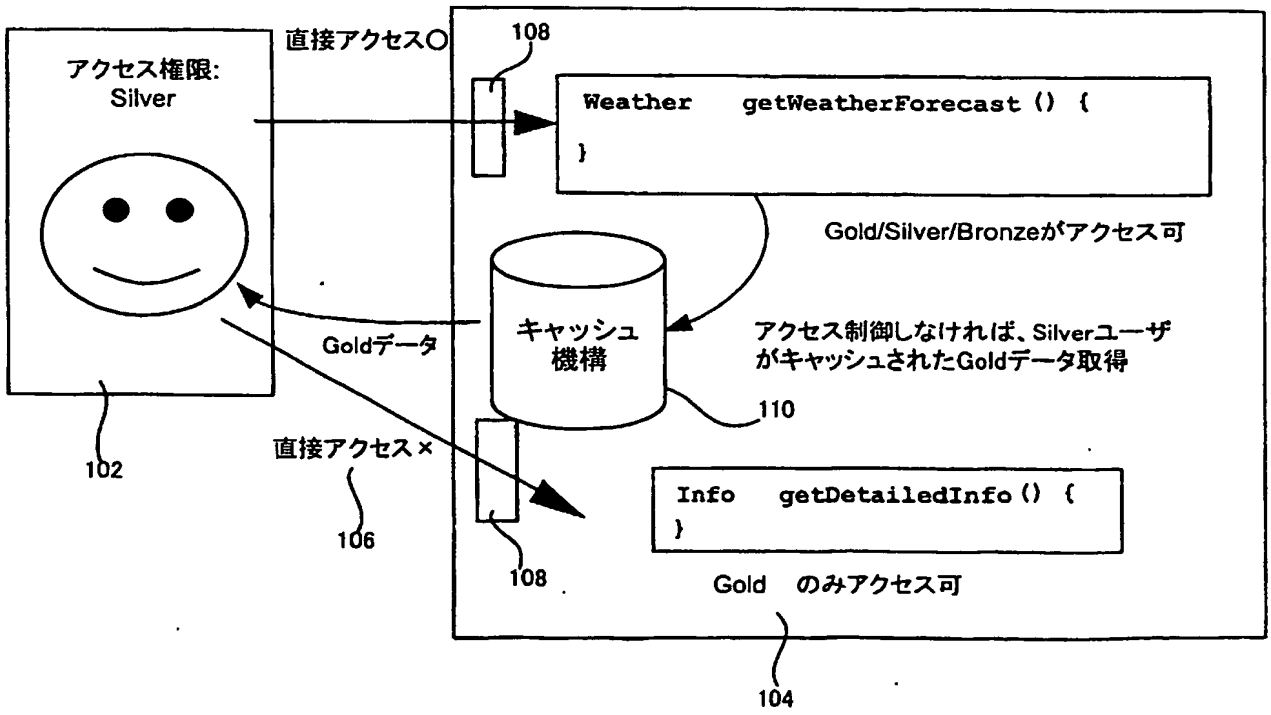
第２０図


Gold/Silver/Bronzeがアクセス可能
104
アクセス権限:
Silver
アクセス不可
アクセス不可
アクセス可
106
Weather getWeatherForecast () {
if (..) .. getDetailedInfo () ..
}
Info getDetailedInfo () {
}
Goldのみアクセス可能
Weather getRoughWF () {
}
Gold/Silver/Bronzeがアクセス可能
102

第２１図


アクセス権限:
Silver
108
アクセス制御
Weather getRoughWF () {
}
Gold/Silver/Bronzeアクセス可
応答遅延
Info getDetailedInfo () {
}
Goldのみアクセス可能
106
104
102

第２２図


直接アクセス○
108
アクセス権限:
Silver
Weather getWeatherForecast () {
}
Gold/Silver/Bronzeがアクセス可
キャッシュ機構
Goldデータ
アクセス制御しなければ、Silverユーザがキャッシュされたデータ取得
110
直接アクセス×
Info getDetailedInfo () {
}
Gold のみアクセス可
102
106
108
104

第２３図

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16130

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, G06F12/00, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, G06F12/00, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-120048 A (Fujitsu Ltd.), 30 April, 1999 (30.04.99), Full text; Figs. 1 to 7 & GB 9805825 A & US 6243719 B	1-20
A	JP 11-175475 A (Nippon Telegraph And Telephone Corp.), 02 July, 1999 (02.07.99), Full text; Figs. 1 to 5 (Family: none)	1-20
A	JP 2001-167032 A (International Business Machines Corp.), 22 June, 2001 (22.06.01), Full text; Figs. 1 to 14 & CN 1305145 A & US 2001-16872 A	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 21 January, 2004 (21.01.04)	Date of mailing of the international search report 03 February, 2004 (03.02.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調査報告

国際出願番号　PCT[redacted]P03／16130

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ'Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１２／００，Ｇ０６Ｆ１２／１４

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ'Ｇ０６Ｆ１５／００，Ｇ０６Ｆ１２／００，Ｇ０６Ｆ１２／１４

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００４年
日本国登録実用新案公報	１９９４－２００４年
日本国実用新案登録公報	１９９６－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ　１１－１２００４８　Ａ（富士通株式会社） １９９９．０４．３０，全文，第１－７図 ＆　ＧＢ　９８０５８２５　Ａ ＆　ＵＳ　６２４３７１９　Ｂ	１－２０
A	ＪＰ　１１－１７５４７５　Ａ（日本電信電話株式会社） １９９９．０７．０２，全文，第１－５図（ファミリーなし）	１－２０

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　２１．０１．２００４	国際調査報告の発送日　03. 2. 2004
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｂ　９４６３ 後藤　和茂 電話番号　０３－３５８１－１１０１　内線　６９０７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2001－167032　A（インターナショナル・ビジネス・マシーンズ・コーポレーション） 2001．06．22，全文，第1－14図 &　CN　1305145　A &　US　2001－16872　A	1－20